

MCWP 2-13
(Coordinating Draft – 17 May 00)

MAGTF INTELLIGENCE DISSEMINATION



U.S. Marine Corps

PCN ??? ????? ??

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

_____ 2000

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-13, *MAGTF Intelligence Dissemination*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence* and MCWP 2-1, *Intelligence Operations* by providing the higher order tactics, techniques, and procedures for MAGTF intelligence dissemination. It is designed for intelligence personnel involved with the direction, planning, development and execution of intelligence dissemination, including both MAGTF command element intelligence personnel and commanders/operations staffs of MAGTF units with a primary intelligence collection and/or production mission.

MCWP 2-13 describes aspects of MAGTF intelligence dissemination operations and activities including doctrinal fundamentals, responsibilities, dissemination methodologies, command and control, supporting communications and information systems support and architectures, formats for various intelligence dissemination means, dissemination and the common tactical picture, planning and execution. MCWP 2-13 provides the information needed by Marines to understand, plan, execute and improve intelligence dissemination operations in support of the MAGTF.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

JOHN E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: ?????????????????

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

MCWP 2-13, MAGTF Intelligence Dissemination

Table of Contents

		Page
Chapter 1.	Intelligence Dissemination Fundamentals	
1001	Introduction to Intelligence Dissemination	1-1
1002	Definitions	1-2
1003	Overview of MAGTF Intelligence Dissemination	1-3
1004	Principles of Intelligence Dissemination	1-7
1005	Intelligence Dissemination Modes	1-12
1006	Overview of MAGTF Intelligence Dissemination Capabilities and Challenges	1-21
Chapter 2.	Intelligence Dissemination Responsibilities	
2001	General	2-1
2002	Commander	2-1
2003	MEF Command Element G-2 Section and the Intelligence Battalion	2-1
2004	Other Command Element Staff	2-13
2005	MEF Major Subordinate Command (MSC) Intelligence Officers	2-14
Chapter 3.	Intelligence Dissemination Methodology	
3001	Overview	3-1
3002	Determine Dissemination Requirements	3-2
3003	Determine Dissemination Form	3-5
3004	Determine Dissemination Mode	3-7
3005	Allocate Resources	3-9
3006	Disseminate the Intelligence and Take Subsequent Action	3-10
3007	Evaluate Dissemination Effectiveness	3-11
3008	Train Personnel in Dissemination Tactics, Techniques, and Procedures (TTP) and SOPs	3-13
Chapter 4.	Intelligence Dissemination Planning	
4001	Dissemination Planning Process	4-1
4002	Identify Dissemination Requirements	4-2

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1	4003	Develop the Information Flow	4-5
2	4004	Intranet Management	4-10
3	4005	Develop the Dissemination Plan	4-12
4	4006	Allocate Resources	4-16
5	4007	Monitor Execution	4-17
6			
7	Chapter 5.	MAGTF Intelligence Dissemination Architectures	
8			
9	5001	Introduction	5-1
10	5002	Background	5-1
11	5003	Intelligence and Related C2 Nodes	5-2
12	5004	External Architectures	5-19
13	5005	MAGTF CIS Architectures	5-19
14	5006	Intelligence CIS Architecture Objectives and Planning Goals	5-19
15	5007	Intelligence CIS Architecture Planning Methodology	5-20
16	5008	Basic Standing Intelligence CIS Requirements	5-24
17	5009	MAGTF Dissemination SOPs, Plans and Orders	5-26
18			
19	Chapter 6.	Intelligence Estimates and Studies	
20			
21	6001	Overview	6-1
22	6002	Intelligence Estimates and Studies	6-1
23	6003	Types	6-2
24	6004	Preparation Principles	6-5
25			
26	Chapter 7.	Intelligence Briefings	
27			
28	7001	General	7-1
29	7002	Purpose	7-1
30	7003	Common Forms of Briefings	7-1
31	7004	Intelligence Information Brief Format	7-2
32	7005	Types of Briefings	7-3
33	7006	Preparation Principles	7-6
34	7007	Intelligence Briefing Methodology	7-6
35			
36	Chapter 8.	Intelligence Reports	
37			
38	8001	Overview	8-1
39	8002	Periodic Summary Text/Voice Intelligence Reports	8-1
40	8003	Graphic Intelligence Reports	8-3
41	8004	Event-Driven Text/Voice Intelligence Reports	8-4
42	8005	Intelligence Reports Plan and Matrix	8-6
43	8006	Intelligence Report Preparation	8-6
44			

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

**Chapter 9. Intelligence Dissemination and Support to the MAGTF's
Common Tactical Picture (CTP)**

9001	General	9-1
9002	MAGTF CTP Concept of Operations	9-1
9003	MAGTF CTP Planning	9-2
9004	Architecture	9-2
9005	Responsibilities	9-5
9006	MAGTF G-2/IOC CTP Responsibilities	9-6

Appendices

Page

A	Glossary	A-1
	Section I. Acronyms and Abbreviations	A-1
	Section II. Definitions	A-
B	References	B-1
C	Intelligence Estimate Format	C-1
D	Intelligence Briefing Formats	D-1
E	Guide to Preparing and Conducting Presentations	E-1
F	Intelligence Reports Formats	F-1
	Section I. INTSUM Format	F-1
	Section II. INTREP Format	F-5
	Section III. BDA Report Format	F-6
	Section IV. MISREP Format	F-8
	Section V. SALUTE Report Format	F-9
	Section VI. RRFI Format	F-10
G	Intelligence CIS Plan Appendix Format	G-1
H	Intelligence Dissemination Planning Checklist	H-1
I	MAGTF Intelligence CIS Architectures	I-1
	Section I. Notional MEF Intelligence CIS Architectures	I-1
	Section II. MAGTF Intelligence, CI and Reconnaissance Radio Nets	I-54
J	Intelligence Reports Matrix Format	J-1
K	Intelligence Dissemination Plan Appendix Format	K-1

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Figures

Page

1-1	The Intelligence Cycle	1-4
1-2	Requirements Satisfaction	1-5
1-3	Intelligence Dissemination Channels	1-16
1-4	Intelligence Dissemination Modes	1-17
1-5	Intelligence Dissemination Forms	1-18
2-1	MEF G-2 Division Principal Staff Officers and Relationships	2-3
2-2	Intelligence Battalion	2-6
2-3	Intelligence Operations Center	2-7
2-4	AC/S G-2's Principal Subordinate Staff Officers and Their Responsibilities	2-9
3-1	Dissemination Methodology	3-1
3-2	Forms and Pathways for Disseminating Intelligence	3-6
4-1	Example, MEF Intelligence Support to Targeting Flow Diagram	4-6
4-2	Example, Intelligence Dissemination Requirements Matrix Format	4-10
4-3	Example, Dissemination Tracking Matrix	4-17
5-1	National Intelligence Support Team (NIST) Capabilities	5-3
5-2	NIST Deployment Cycle	5-4
5-3	Notional Composition of a NIST	5-5
5-4	NIST JWICS Mobile Integrated Communications System	5-6
5-5	Joint Intelligence Architecture	5-9
5-6	MEF CE's CIC and Intel Battalion's IOC Key Elements	5-11
5-7	MEF CE Cross-Functional Cellular Organization and Intelligence Support	5-13
5-8	Intelligence Operations Center Elements and Composition	5-14
5-9	Notional MEF Intelligence CIS Architecture	5-16
5-10	MEF G-2 and Intel Battalion C2 Relationships and MEF Intelligence Support Flow	5-19
5-11	MAGTF Intelligence CIS Planning Methodology	5-21
7-1	Briefing Preparation Steps	7-4
9-1	MAGTF CTP Notional Network Architecture	9-3
9-2	MAGTF CE Main Command Echelon Notional Network Architecture	9-4
I-1	MEF CE Combat Intelligence Center and Intelligence Battalion IOC GENSER Systems Architecture	I-3
I-2	MEF CE Combat Intelligence Center and Intelligence Battalion IOC – SCI Systems Architecture	I-6
I-3	Intelligence Bn IOC J-STARS CGS Architecture	I-8
I-4	MEF CE and Radio Battalion OCAC Architecture	I-11
I-5	Intelligence Bn Imagery Intelligence Platoon Architecture	I-13
I-6	Intelligence Bn IOC Surveillance and Reconnaissance Cell	I-16
I-7	Radio Battalion C2, Operations & Collection Systems Architecture	I-18

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Figures (cont.)

Page

I-8	Topographic Platoon, Intelligence Bn, Architecture	I-20
I-9.	CI/HUMINT Company, Intelligence Battalion, Architecture	I-22
I-10	Ground Sensor Platoon, Intelligence Battalion, Architecture	I-24
I-11	Division Main Command Post Combat Intelligence Center GENSER Architecture	I-11
I-12	Division Main Command Post Combat Intelligence Center Sensitive Compartmented Information Architecture	I-29
I-13	Reconnaissance Battalion Reconnaissance Operations Center and Light Armored Reconnaissance Battalion COC Architectures	I-31
I-14	Marine Aircraft Wing Air Combat Intelligence Section GENSER Architecture	I-33
I-15	Marine Aircraft Wing Air Combat Intelligence Section SCI CIS Architecture	I-35
I-16	VMAQ Squadron Architecture	I-37
I-17	VMU Squadron Architecture	I-39
I-18	FSSG Headquarters Combat Intelligence Center Architecture	I-41
I-19	Combat Service Support Detachment Architecture	I-43
I-20	MEU(SOC) Amphibious Task Force Intelligence Center CIC Architecture (Afloat)	I-45

Tables

Page

I-1	MEF CE CIC and Intelligence Battalion IOC GENSER Systems and Communications Interface Requirements	I-4
I-2	MEF CE CIC and Intelligence Battalion IOC SCI Systems and Communications Interface Requirements	I-7
I-3	Intelligence Bn IOC J-STARS CGS Systems and Communications Interface Requirements	I-3
I-4	MEF CE and Radio Battalion OCAC Systems and Communications Interface Requirements	I-12
I-5	Intelligence Bn Imagery Intelligence Platoon Systems and Communications Interface Requirements	I-14
I-6	Intelligence BN IOC SARC Systems and Communications Interface Requirements	I-17
I-7	Radio Battalion C2, Operations & Collection Systems Interface and Communications Requirements	I-19

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Tables (cont.)

Page

I-8	Topographic Platoon Systems and Communications Interface Requirements	I-21
I-9	CI/HUMINT Company Systems and Communications Interface Requirements	I-23
I-10	Ground Sensor Platoon Systems and Communications Interface Requirements	I-25
I-11	Division Main Command Post CIC GENSER Systems and Communications Interface Requirements	I-27
I-12	Division Main Command Post CIC SCI Systems and Communications Interface Requirements	I-30
I-13	Reconnaissance Battalion Reconnaissance Operations Center and Light Armored Reconnaissance Battalion COC Systems and Communications Interface Requirements	I-32
I-14	Marine Aircraft Wing Air Combat Intelligence Section GENSER Intelligence Systems & Communications Interface Requirements	I-34
I-15	Marine Aircraft Wing Air Combat Intelligence Section SCI Systems and Communications Interface Requirements	I-36
I-16	VMAQ Squadron Systems and Communications Interface Requirements	I-38
I-17	VMU Squadron Systems and Communications Interface Requirements	I-40
I-18	FSSG CIC Systems and Communications Interface Requirements	I-42
I-19	Combat Service Support Detachment Systems and Communications Interface Requirements	I-44
I-20	MEU(SOC) ATFIC CIC GENSER System and Communications Interface Requirements	I-46
I-21	MEU(SOC) ATFIC CIC SCI System and Communications Interface Requirements	I-46
I-22	Standard Communication Pathways and Connectivity	I-47

Chapter 1

Intelligence Dissemination Fundamentals

1001. Introduction to Intelligence Dissemination

a. **Objectives.** Intelligence has two objectives: to reduce uncertainty and to assist in protecting friendly forces through counterintelligence (CI). *The objective of intelligence dissemination within the Marine Air Ground Task Force (MAGTF) is to quickly and securely deliver relevant intelligence to tactical commanders and those who need it, in a timely manner and usable format, to satisfy their planning and decisionmaking needs.*

b. **The Balance.** Effective intelligence dissemination requires that intelligence personnel have exceptional situational awareness not only of enemy capabilities and probable courses of action, but also of friendly missions, the commanders' intent, and concepts of operations. It also requires intelligence personnel to display good judgment. *Too much or too little intelligence can adversely affect operations.* Successful intelligence dissemination reduces uncertainty and friction, enhances situational awareness, and results in a smarter fighting force on the battlefield.

c. **The Challenge.** MAGTF intelligence dissemination requires planning, management, and flexibility for successful execution. With the fielding of numerous operational and intelligence-related automated systems, as well as the challenges of joint, combined, and allied operations, MAGTF intelligence dissemination has become a complicated endeavor. *Yet systems planning alone is not enough. Planning and executing intelligence dissemination is both an art and a science, full of trade-offs and risks.* Mastery of intelligence dissemination principles alone will not suffice; these techniques and procedures must be fully integrated with intelligence collection and production, and applied creatively to achieve success.

Skill and initiative factor into successful MAGTF intelligence dissemination operations. If intelligence personnel have operational and tactical situational awareness, they can overcome deficiencies in the dissemination architecture through personal initiative and perseverance. They will know when a unit or section outside of "normal distribution" needs certain intelligence, use appropriate alternate means of dissemination (when necessary), and make sure the intelligence is disseminated, received and understood.

1002. Definitions

- a. Intelligence.** 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Knowledge about the enemy or the surrounding environment needed to support decision making. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02) Also, in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)
- b. All-Source Intelligence.** Intelligence products and/or organizations and activities that incorporate all available sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (Joint Pub 1-02)
- c. Intelligence Requirement (also called IR).** Any subject, general or specific, upon which there is a need for the collection of information or the production of intelligence. (Joint Pub 1-02) In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (MCRP 5-12C)
- d. Intelligence Dissemination.** Conveyance of intelligence to users in a suitable form. (Joint Pub 1-02)
- e. Intelligence Requirements Management (IRM).** Encompasses the continuous evaluation of the importance of each developed intelligence requirement within the context of the operational mission and enemy activities; the information and assets needed to satisfy each; the resources presently committed toward fulfilling these; the supporting command, control, communications and computer (C4) support system for the transmission of information and intelligence; and the degree to which each has been satisfied by completed intelligence activities. (MCWP 2-1) Key components of requirements management are intelligence collection management (ICM), intelligence production management (IPM), and intelligence dissemination management (IDM).
- f. Dissemination Management --** Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12)

g. Commander's Critical Information Requirements (CCIRs). Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirements; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

h. Priority Intelligence Requirements (PIRs). Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. (Joint Pub 1-02) In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

1003. Overview of MAGTF Intelligence Dissemination

a. General. Dissemination involves establishing dissemination priorities, selecting dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to all appropriate users in the proper forms, at the right times, while ensuring that individual users and the dissemination systems are not overloaded by irrelevant intelligence and information. Dissemination also provides for use of security controls that do not impede the timely delivery or subsequent use of intelligence while providing appropriate protection of intelligence sources and methods.

The dissemination system must ensure sufficient streamlined communications and information systems (CIS) connectivity with all supporting intelligence resources and be integrated with internal intelligence as well as the broader operational command and control (C2) structure. From national and theater echelons, throughout the joint force and the MAGTF, all-source intelligence pertinent to tactical operations must be identified, quickly retrieved, processed, tailored to the supported echelon, and ultimately made available to planners and decisionmakers at all MAGTF command echelons in time to be of value to their operations.

b. Intelligence Dissemination and Intelligence Functions. In providing support to the commander, MAGTF intelligence operations must support six specific intelligence functions:

- Support to the commander's estimate
- Situation development
- Indications and warning (I&W)
- Support to force protection
- Support to targeting
- Support to combat assessment

Intelligence dissemination is vital to all these functions, for intelligence is meaningless unless it reaches the right people in time to affect the decisionmaking process and in a form that is understandable. (MCWP 2-1) Whether disseminated electronically, by hard copy, verbally, or via courier, effective intelligence dissemination provides intelligence to all users in a timely fashion.

c. Intelligence Dissemination within the Intelligence Cycle. The process used to develop intelligence is called the intelligence cycle. (See figure 1-1) The intelligence cycle consists of six sequential yet interdependent steps: planning and direction; collection; processing and exploitation; production; dissemination; and utilization.

Dissemination is equal in importance to any other intelligence cycle activity. Without dissemination, commanders do not receive the intelligence products needed for the planning and execution of operations. During MAGTF operations, intelligence dissemination must be planned for and supervised *to the same degree* as collection, processing and production to ensure that intelligence operations and intelligence support are successful.

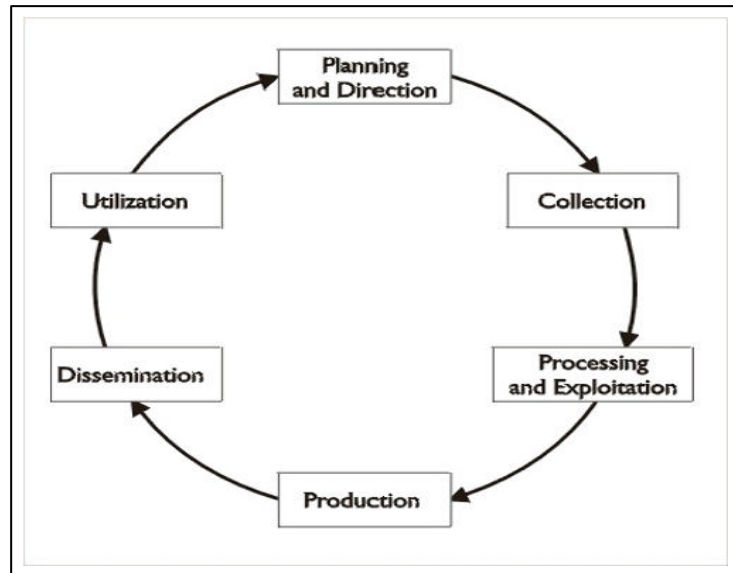


Figure 1-1. The Intelligence Cycle

d. Basic Dissemination Management Process

(1) General. Intelligence dissemination management is the process that helps identify and validate intelligence dissemination requirements, prioritizes these, determines effective

means for acquiring information and previously produced intelligence to help satisfy these, and develops and supervises internal intelligence dissemination and CIS operations executed to accomplish this. First, intelligence dissemination must be done in an integrated manner with intelligence collection and intelligence production management, all within the framework of intelligence requirements management. Then, beyond its critical tie to requirements management, dissemination requires the skills and flexibility mentioned earlier – for even the best planning cannot predict with certainty who will need what across all aspects of the operation.

(2) Requirements Management. Requirements management planning is the first step in dissemination planning. In MAGTF intelligence operations, intelligence collection, production, and dissemination all flow out of an integrated intelligence planning and direction process that is built upon IR management. Each IR will generally have an associated intelligence collection requirement (ICR), intelligence production requirement (IPR), and intelligence dissemination requirement (IDR).¹ (See figure 1-2.)

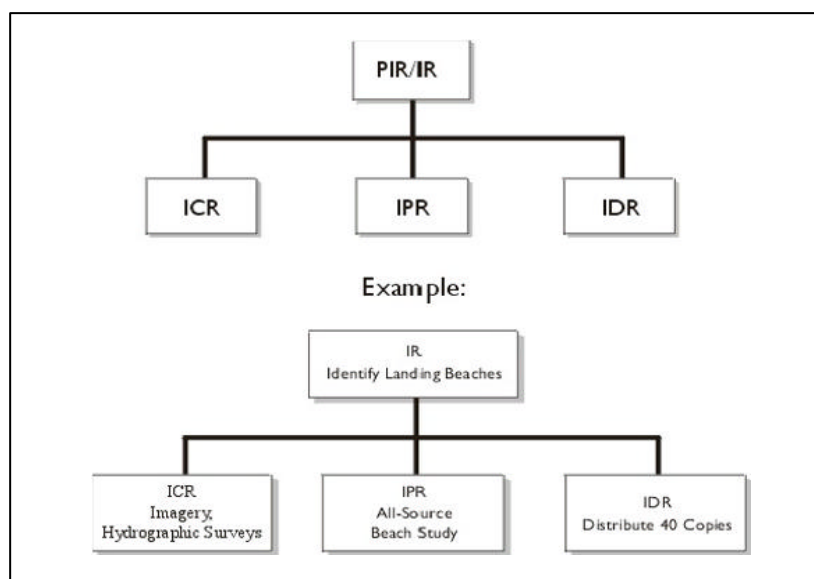


Figure 1-2. Requirements Satisfaction

¹ For more discussion of requirements management, see chapter three of this publication and MCWP 2-1 *Intelligence Operations*, chapter three.

(3) Dissemination Management Functions. There are two distinct functions within dissemination management: dissemination *requirements* management; and dissemination *operations* management. Dissemination requirements management defines *what* intelligence will be disseminated and *who* needs it, and dissemination operations management specifies *how* the intelligence will be disseminated. They are considered separately to better understand their objectives, but in practice the distinction between them often disappears.

(a) Dissemination Requirements Management. Dissemination requirements management is driven by the dissemination strategy, which incorporates commander's intent, PIRs, IRs, concept of operations and requests for intelligence (RFIs). Developing a dissemination strategy ahead of time pays dividends by familiarizing personnel with which intelligence products will be disseminated by what means, describing alternate means of dissemination, and providing all MAGTF users with information they need to ensure they have the right dissemination SOP, architecture and training.

(b) Dissemination Operations Management

(1) Means. Delivery of the intelligence product to MAGTF users is directly related to the choice of the means used to disseminate that product. Dissemination is managed by using a combination of methods (supply-push and demand-pull), channels (standard and alarm), and modes (broadcast and point-to-point) to convey the product to users. These means are discussed in detail in paragraph 1005.

(2) Architectures. How the intelligence is disseminated is a function of the status of dissemination systems (both automated and manual) and alternate means. The functioning of MAGTF CIS circuits, such as Marine Expeditionary Force (MEF) radio nets and Secret Internet Protocol Router Network (SIPRNET) connectivity, are the responsibility of the CIS officer (G/S-6); dedicated intelligence systems vary in who is responsible for their operation.

(3) Responsibility. Regardless of the status of intelligence dissemination CIS support and connectivity, the intelligence officer is responsible for timely dissemination of critical intelligence. Intelligence personnel must be able to quickly and reasonably determine how and to whom to disseminate critical intelligence when planned dissemination flow is degraded or interrupted.

Dissemination requirements management and dissemination operations management are performed at all levels of the intelligence community. At the MAGTF command element (CE) it is coordinated by the intelligence battalion in accordance with the MAGTF G/S-2's direction. However, each element of the MAGTF performs dissemination management functions. Each unit interacts with levels above and below, and among units, organizations, and agencies on the same level. The further up the chain of command, the broader the perspective and scope of responsibility; the lower, the more specific the function and narrow the scope.

(4) **Dissemination Process.** Integrating intelligence dissemination efforts with those of collection, processing, and production is an ongoing process. Dissemination planning and direction begins with the receipt of an IR and encompasses the following series of steps, discussed in detail in chapters 3 and 4 of this publication:

- Identification of IRs
- Determination of dissemination priorities and forms
- Selection of means to deliver intelligence
- Allocation of resources
- Intelligence dissemination
- Monitoring the flow of intelligence

1004. Principles of Intelligence Dissemination

In order for intelligence to be of value to tactical commanders, it must meet the following basic dissemination requirements:

Pertinence, Usability of Form, Timeliness, and Security.

a. Pertinence. The dissemination system must provide the flexibility to use a *supply-push* system (which pushes important or time-sensitive intelligence directly to users), while also permitting users to *demand-pull* other relevant intelligence as needed from readily accessible sources, such as a database or a watch section at an intelligence center.

(1) Requirements. *Relevant intelligence must be disseminated to all units or agencies that require it.* Determining who gets what is the real “art” part of dissemination. It gets back to identified IRs, which necessitates thorough knowledge and understanding of user needs and missions based on the current situation, commanders’ intent, and PIRs. In short, intelligence must be tailored to the needs of the commander/planner.

Intelligence personnel must know and understand each user’s PIRs and other IRs; however, being tactically aware is equally important. PIR lists will not cover all the bases of intelligence needs: they just can’t. These requirements are a minimum, and they change. Tactical judgment is important -- *disseminate pertinent intelligence, whether the requirement is on a PIR list or not.*

(2) **Intelligence and Information.** Intelligence is not simply another term for information. Intelligence is more than an element of data or a grouping of information; it is a body of knowledge. There is a clear and important distinction between raw data, information, and intelligence. To be considered intelligence, data must be placed in context to provide an accurate and meaningful image of the hostile situation.

Intelligence staffs process acquired information into usable intelligence, tailor the product for consumers, and disseminate it. The guiding principle is to disseminate *intelligence*, not simply *information*, to supported decisionmakers. **However:**

- ***Disseminating information, not just intelligence, is important.*** Because of their highly perishable or critical nature, combat data (derived from reporting by operational units) and sensor data are sometimes used to effect decisions without being converted into intelligence, especially in support of target acquisition operations. A caution: this type of data and information is not evaluated intelligence. Thus, this area has the potential for over-reactive targeting, since it may lead to immediate operational reaction based on information, not processed intelligence. Like other critical flash warnings, combat and sensor data may later be explained in ways other than the original assumption. Additionally, this type of information has the potential to be over-disseminated. Operational rules of engagement must match the command's reactive targeting policy. The G/S-2 must coordinate closely with the G/S-3 (for responsibilities) and the G/S-6 (for bandwidth, connectivity, and time-sensitivity aspects) to develop procedures for these issues.
- ***Additionally, crisis situations may preclude some or all of the normal filtering process.*** Filtering is a responsibility shared among intelligence collectors, producers and disseminators, as well as among intelligence and other warfighting functional personnel.

When time-sensitive crisis situations preclude deliberate intelligence processing and necessitate dissemination of untailored intelligence or unevaluated information, intelligence personnel must ensure that tactical commanders are aware that they are receiving unevaluated intelligence.

(3) **Downward Dissemination.** *Generally, dissemination downward should be selective.* Units should not receive irrelevant intelligence or voluminous amounts of information which tie up their communication channels. This is especially valid in the case of dissemination to lower tactical units whose capabilities for processing and producing information are relatively limited. However, broad dissemination which results in the occasional delivery of intelligence to a unit to which it is not pertinent is preferable to selective dissemination in which units may

fail to receive

available intelligence when they need it. *If doubt exists, disseminate the intelligence.* Just be sure to minimize the doubt factor through good situational awareness and tactical judgment.

(4) Upward and Lateral Dissemination. Conversely, *greater quantities of intelligence are generally disseminated upward and laterally* because the pertinence of intelligence to such units/echelons may be broadly affected by a change in the situation. This is particularly true for intelligence regarding battle damage assessment (BDA), that of potential value to future operations, and that critical to exploitation of threat vulnerabilities requiring immediate higher headquarters' operational decisions and actions. An item of intelligence which is not needed by a particular unit at a given time may prove pertinent to it later or may be extremely important to an adjacent or senior unit. *Again, if doubt exists as to whether to disseminate an item, disseminate the intelligence.*

(5) General Guidance. Satisfying the pertinence attribute requires intelligence Marines to master two general challenges:

(a) Situational Awareness and Current IR Priorities. First, they must maintain constant and accurate awareness of the operational situation and of current intelligence requirements priorities. In doing so, they must avoid a natural tendency to focus solely upon their own command echelon's requirements and activities, to the neglect of the broader force -- particularly those of subordinate and lateral units.

(b) CIS System Status Awareness. Second, they must stay current on the status of the supporting CIS: which links and networks are operational; which are being excessively taxed; which are available for immediate time-sensitive needs; how all users can be reached quickly when required; etc. By doing so, their ability to anticipate situations within a dynamic operational environment enhances responsiveness and improves the ability to disseminate specific intelligence to those for whom it is relevant.

b. Usability of Form. *Disseminated intelligence must be in a form suitable for immediate use by the recipient and should be tailored as much as possible for the intended consumer.* The tactical commander should be able to quickly identify and apply relevant intelligence without additional analysis or manipulation. Standard formats, such as the intelligence estimate, intelligence studies, briefings, reports, etc., must be established, understood, and practiced by intelligence personnel and users. *When appropriate*, intelligence personnel should limit textual data and employ graphics to reflect and disseminate intelligence. This helps convey an accurate *image* of the battlespace or threat to the decisionmaker in a form that aids his rapid understanding of the intelligence. It's important to remember, however, that different units and echelons have different capabilities and requirements -- e.g., some may prefer having access to datastreams and databases (instead of graphics).

Dissemination methods, channels, modes and forms will vary according to the situation, the location of the recipient, the urgency of the intelligence, the complexity or nature of the intelligence, the disseminating and receiving intelligence sections' capabilities, and the available dissemination means.

- **Written documents** -- intelligence estimates, OPLAN/OPORD annexes, studies and reports -
- are useful for general dissemination of large amounts of intelligence to many users,
particularly within larger organizations (when time is not critical and when deliberate
planning is possible) and for all organizations in support of specified wartime contingency
planning.
- **Messages** -- both textual and voice -- may be effective for either routine or time-critical
situations, particularly if restricted to a single intelligence subject, issue, or action. It is
important, however, that formats be standardized and understood by all -- particularly if
abbreviations or codes are used to aid with brevity.
- **Oral briefings** -- especially when built around a situation map and focused supporting
graphics and imagery -- are often used during deliberate planning as well as during dynamic
and time-sensitive operations, and are the norm for intelligence dissemination to the
immediate commander and his staff.

Automated technologies and "information systems" -- are advancing opportunities for
intelligence personnel at all command echelons to employ capabilities such as *demand-pull*,
video-conferencing and *enhanced graphical techniques* to access broad intelligence
community resources that incorporate each of the previous methodologies. The increasing use
of world-wide web (www) like technologies is one such example.

c. Timeliness. *Intelligence must be disseminated in time to influence planning, decisionmaking and execution or it is worthless. In particular, fast dissemination of critical, time-sensitive intelligence and related information is vital.* Timely intelligence concerning enemy capabilities and intentions is critical to the formulation of sound tactical decisions and, ultimately, to mission success. The commander's intent, once formulated, guides intelligence staffs in identifying PIRs and anticipating future IRs. A continuous interaction between intelligence and operations personnel and access to intelligence organizations, systems and products assists in the performance of effective intelligence dissemination.

(1) Factors Influencing Timely Dissemination. Many factors influence intelligence timeliness. The sheer volume of intelligence reporting, especially in a crisis, can sometimes degrade the performance of available intelligence communication networks and overwhelm

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

scarce analytical resources. Distance, mobility and terrain factors often limit available CIS options, such as automated wide area networks (WANs), thereby increasing reliance upon less effective single channel radio and courier methods. Other factors include the communications means available; the quality of the intelligence (i.e., acquired information usually needs some level of analysis before it can be of use to recipients); the quantity and quality of intelligence previously disseminated; and the need to properly reformat certain intelligence products (in user-friendly formats) before they can be further disseminated. Additionally, a heightened tempo usually produces a greater quantity of IRs and a larger customer base than normal. Finally, hardware and software requirements may pose interoperability or security problems – especially in joint or multinational operations.

(2) Date Desired (DATEDES). Date-time-group of when the requester requires the intelligence product.

(3) Latest Time Intel of Value (LTIOV). LTIOV should be designated in cases where the intelligence value of intelligence collection would still be of use even if received after the specified date desired. LTIOVs should be written into PIRs for incorporation into dissemination operations planning and management.

(4) Planning Factors. Intelligence dissemination plans and procedures must incorporate:

- IDR priorities, to include integrated linkage with ICRs and IPRs.
- Preferred intelligence product formats (e.g., by unit or staff section).
- Primary and alternate communication means with all supported units.
- Routine and time-sensitive means and responsibilities.
- Procedures to positively verify that the intelligence has been received by the intended recipients.

Intelligence dissemination should be preplanned, tailored and automated to the degree possible. Back-up plans and manual means of dissemination must also be developed and planned for. To ensure quality dissemination, intelligence personnel should tailor intelligence for specific recipients as much as possible – based on unit mission. Finally, *if critical information is received that will affect operations, it should be passed on immediately without processing. Do not sacrifice timeliness to allow more analysis if the intelligence may be critical!*

(5) Improving Timely Dissemination. To improve timely intelligence dissemination:

- Assign priorities to intelligence requiring dissemination.
- Target specific recipients for each intelligence product.
- Reduce volume.
- Develop well-defined procedures that are understood by all.
- Train.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 **d. Security.** *There will always be a trade-off/tension between security and dissemination.*

2 *Intelligence should be disseminated by any system available that provides adequate*
3 *information security.* This includes secure communications such as voice, facsimile, radio,
4 video, teletype, wire, computer, and the VHF/UHF/SATCOM links. The purpose of
5 transmitting intelligence securely is to preclude the enemy from knowing the sources and
6 effectiveness of MAGTF intelligence operations and then altering his actions or strengthening
7 his counterintelligence (CI) efforts.

8
9 Security extends beyond simply the intelligence battlespace activity. It must be planned for and
10 integrated with the full scope of current and future command security program activities:
11 operations, information, communications, personnel and physical security. The goal is simple:
12 keep the enemy from exploiting any friendly security vulnerability in a manner that allows him
13 to gain planning, decisionmaking and operational tempo advantages over ours.

14
15 **(1) Available Secure Tools.** The majority of tactical communications and information
16 systems used today have integral or supporting features that provide sufficient security
17 protection. For more restricted operational (e.g., focal point) or sensitive compartmented
18 information (SCI) communications, detailed procedures exist that allow for sanitization and
19 timely broader dissemination whenever necessary. Accordingly, the principal security challenge
20 that may be faced during tactical or crisis situations is when events occur which disrupt or
21 degrade these unit CIS, necessitating a potential trade-off between security and dissemination.
22 Similarly, the increasing frequency of multinational operations raises an additional
23 dissemination challenge regarding the sharing of intelligence among allied and coalition forces.

24
25 **(2) Considerations.** *Tailored intelligence will be disseminated via the best means*
26 *available consistent with the operational situation.* Although by nature most intelligence will be
27 classified, even some unclassified intelligence may require security protection due to operational
28 security considerations. Resolving these challenges will be situationally dependent -- there is no
29 rule of thumb covering all possibilities. Relevant factors to consider include:

- 30
31
 - The enemy's own intelligence collection, processing and dissemination capabilities.
 - 32 • Phase of the operation's planning or execution.
 - 33 • Significance of current intelligence gaps, particularly at lower tactical units.
 - 34 • How the intelligence may support the dynamic and timely exploitation of threat
 - 35 vulnerabilities and tactical opportunities.

36
37
38 **(3) Urgent Situations.** The standing principle is to use secure dissemination methods
39 whenever possible. However, **if doubt exists and the situation and intelligence are time-**
40 **sensitive, disseminate the intelligence via any available means!** In such cases, immediately
41 inform the unit security manager and intelligence officer, who will then assess any possible
42 damage and initiate necessary remedial corrective actions.

1005. Intelligence Dissemination Modes. Delivery of tailored intelligence products and other support to the right people in a timely manner is directly related to the means of dissemination. Within the MAGTF, no single way of disseminating will be satisfactory for all recipients and for all situations -- a combination of *methods, channels, modes and forms* are planned, managed and employed to accomplish the intelligence dissemination goal.

a. Dissemination Methods

There are two basic methods used to disseminate intelligence: Supply-Push and Demand-Pull. The key factors influencing which dissemination mode is chosen are: supported PIR/IR, timeliness, recipient, and format. Intelligence planners must develop and implement intelligence dissemination plans with the flexibility to exploit either methodology, pushing time-sensitive intelligence directly to users while simultaneously allowing them to pull other intelligence as needed.

(1) Supply-Push. The supply -push method disseminates intelligence as it becomes available (or on a schedule) from the intelligence collector/producer down to selected users to satisfy their IRs or to relay other relevant intelligence information (e.g., status update on planned intelligence collection operations). This method is said to be "need-driven" -- the delivery of intelligence is triggered by the availability of that intelligence and understanding of its need by specific users.

and updates to schedules, distribution lists, databases or overlays.
Electronic and hardcopy messages, e-mail, voice, and fax are used to disseminate supply-push intelligence.

6/5/00

Advantages. The key advantage is that users do not have to initiate requests to receive intelligence support or products.

Disadvantages. Its key disadvantage is the potential for information overload -- either of the CIS support architecture or of the user's ability to process a large amount of intelligence in a timely manner. Thus, *for supply-push methods, the disseminator must strive to tailor the intelligence to specific users, and not simply broadcast it to a large audience. Likewise, users should take themselves off distribution for intelligence products they don't need.*

(3) **Demand-Pull.** This method seeks to exploit technological improvements by giving users either direct electronic access to intelligence databases, files, servers or other intelligence products and repositories through detailed search or inquiry procedures, or via direct queries to intelligence planners' and producers' watch sections, such as the MEF's Production and Analysis (P&A) Cell or, through reachback, to the Joint Intelligence Center (JIC).

Demand-pull dissemination also results from unanticipated needs by a commander and his staff and can flow up, down, or laterally through the G-2 intelligence and CIS architectures. This type of dissemination occurs primarily when there is a need by a lower command echelon to access intelligence archives at higher headquarters--such as databases and technical files maintained at JICs and the P&A Cell--for amplifying intelligence to support its planning activities, such as basic/descriptive intelligence or technical information. It also, however, may be employed by higher echelons to satisfy IRs when the amplifying data can best be acquired from subordinate units.

Examples. Standard intelligence reports and products scheduled for release at standard times (such as INTSUMs, DISUMs, and weather reports) can be efficiently disseminated via the MAGTF intelligence website, with hardcopy/courier dissemination as the alternate means. Most often, intelligence products and data are posted on a computer server for users to view, then download as needed. Examples of demand-pull dissemination means include INTELINK, image product library (IPL) servers, websites and databases. CIS connectivity may be either the standard MAGTF tactical data network (TDN) or by dedicated intelligence CIS.

7/5/00

Advantages. The advantage of demand-pull dissemination is that it may significantly reduce the volume of intelligence being transmitted through the MAGTF TDN, particularly regarding intelligence with no immediate influence on the current battle. Further, it allows users to better employ their intelligence processing and production capabilities by reducing their receipt of superfluous intelligence products. It also contributes to the preparation of better tailored products for the commander.

Disadvantages. Demand-pull intelligence dissemination can be more time-consuming than supply-push modes. Its main disadvantage, however, is that intelligence timeliness may be degraded in that the user may not receive critical intelligence until he after he has initiated a request for it. Additionally, the generally more limited area of interest (AOI) of lower echelon units may lead to situations where they are ignorant of available intelligence of value to future operations. Finally, users must know in advance where all desired intelligence products may be accessed in order to support immediate use.

b. Channels

Intelligence is disseminated using two types of channels: Standard and Alarm.

(1) **Standard Channels.** Standard dissemination consists of a transmission of intelligence down and laterally through the chain of command according to a set order and format. It is used for routine intelligence dissemination (to maintain and share situational awareness and current intelligence of the battlespace) and is the channel used for the majority of dissemination requirements. Dissemination generally occurs on a regular schedule or intervals. Examples of standard intelligence dissemination include studies, reports, routine message intelligence summaries and formal staff briefings. Standard dissemination employs normal MAGTF command and staff channels and the supporting CIS.

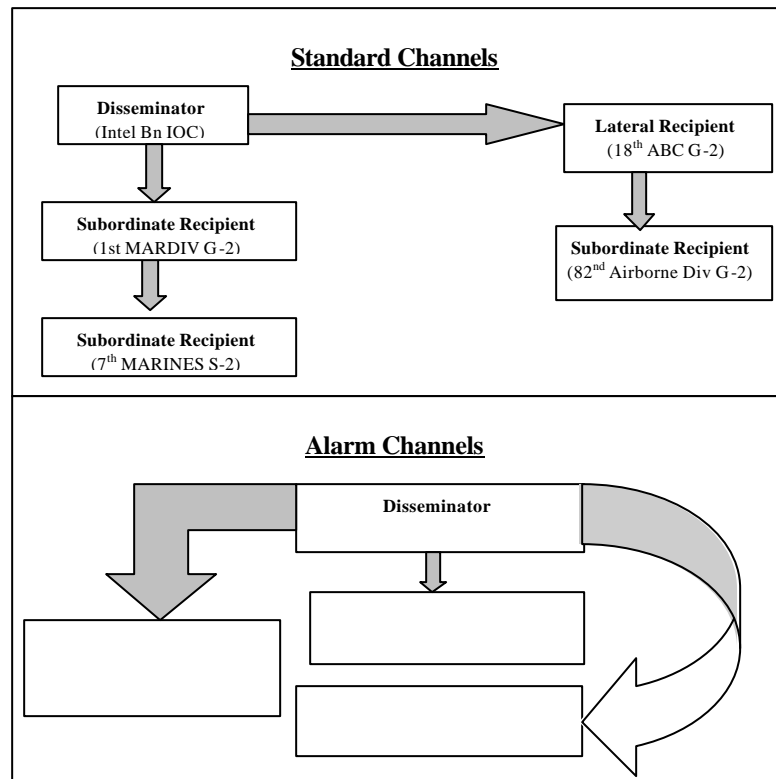
(2) **Alarm Channels.** Alarm channel dissemination is used for critical, time-sensitive intelligence that can have an immediate effect on operations. This type of dissemination has

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

no set format or schedule and activates only when critical intelligence is received that requires immediate decision or action, and thus rapid dissemination. When an alarm-triggering event occurs, intelligence must go to the units or sections most affected by the most direct means possible, even if it means skipping echelons of command. CIS connectivity may be either the standard MAGTF CIS architecture or by dedicated intelligence CIS. Because alarm intelligence is time-sensitive, dissemination should include a means for verifying receipt and understanding. Intelligence operations reporting criteria and supporting dissemination procedures must ensure that filters and thresholds for alarm-triggering events are developed, understood, and practiced in advance. Effectively disseminating intelligence via alarm channels requires:

- Detailed intelligence collection, production and reporting direction.
- Broad MAGTF CIS knowledge.
- Frequent multi-echelon training (to include other service and joint organizations).
- Training for intelligence, operations and unit personnel operating CIS systems to improve their ability to immediately recognize, act upon received intelligence, and disseminate it.



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

Figure 1-3. Intelligence Dissemination Channels

c. Dissemination Modes. Intelligence is disseminated via one of two modes: *Broadcast or Point-to-Point*.

(1) Broadcast Mode. When using the broadcast mode, intelligence that affects the majority of units is disseminated simultaneously to a broad audience. Common examples are the dissemination of the initial MAGTF intelligence estimate developed during contingency planning, or the dissemination of an I&W report of an enemy surface-to-surface missile launch. Successful use of broadcast modes depends upon several factors: judicious selection of what intelligence is disseminated; the ability of all pertinent users to monitor the broadcast; and as technology improves and new systems are fielded, the availability of a processing methodology to filter and select for detailed examination only that intelligence pertinent to user requirements. This mode offers the advantage of improving dissemination timeliness, but only if used with discipline, due to the risk of overloading MAGTF CIS pathways or burdening lower units' intelligence processing capabilities.

(2) Point-to-Point Mode. In the point-to-point mode, intelligence is disseminated to a specific user(s), normally in response to previously stated IRs. From there it may be further disseminated by users to others as appropriate. Although this mode is generally slower than the broadcast mode, it allows for more intelligence focus and tailoring to specific user needs in that each recipient acts as a sort of control mechanism, filtering and integrating intelligence prior to disseminating it further, thereby reducing information overload of others with unnecessary intelligence. Conversely, this very control mechanism adds another risk as the intelligence

meaning may become distorted as it is conveyed from one command to another. Examples of point-to-point modes include e-mail, voice radio or telephone, and courier. When a secure WAN or local area network (LAN) is operational, a majority of intelligence disseminated between the MEF and its major subordinate commands (MSCs) may be via email. Below the MSC level, the majority of point-to-point dissemination is done either by radio, wire communications or courier.

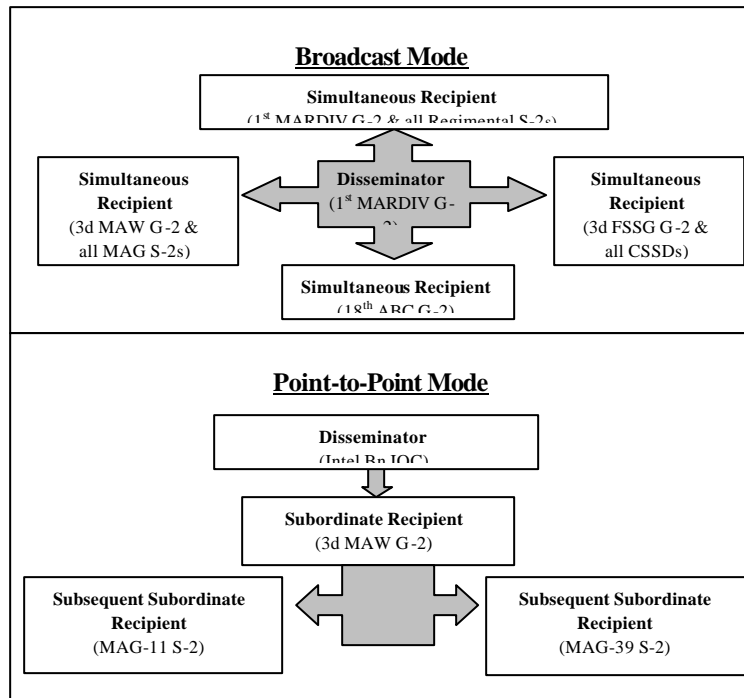


Figure 1-4. Intelligence Dissemination Modes

d. Dissemination Forms

Intelligence may be disseminated in a variety of forms. Formats may be either stand-alone or employed in combination with each other, and are categorized as: Verbal Documents, Electronic, or Graphical.

6/5/00

The most suitable format for intelligence dissemination depends primarily on the needs of the commanders and planners, the nature and urgency of the intelligence and the means available to convey the information. Which is most suitable depends primarily on the user's requirements -- which the unit intelligence officer should always consciously consider and specify whenever stating an intelligence production and/or intelligence dissemination requirement.

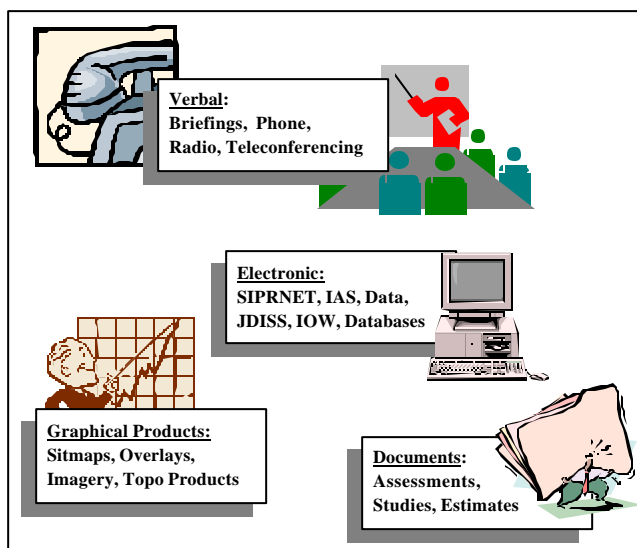


Figure 1-5. Intelligence Dissemination Forms

(1) Verbal. Examples include dissemination via radio or telephone; face-to-face, such as during formal or informal intelligence briefings or the constant intelligence/commander/staff personal interaction; or a more recent combination of these in the form of video-teleconferencing. The primary benefit of verbal formats is timeliness (both in getting the information to the user, and by the disseminator having immediate positive verification of delivery) and the possibility for immediate feedback or questioning, particularly during fast-developing situations. Additionally, it can enhance communication in that many more subtle factors -- tone of voice, inflection, facial expressions, body language, gestures -- may convey deeper meaning and understanding than the words alone could. Disadvantages of verbal formats are difficulty in conveying and ensuring understanding (particularly if the subject is complicated) concurrently to a large audience; and the risk that the recipient may assume understanding, when in fact he does not, and fail to ask questions or seek necessary clarification.

Briefings

Intelligence briefings are used extensively to provide both background and situation data and can range in scope from fairly lengthy and complex presentations of technical data to one-minute enemy situation and order-of-battle updates. Dissemination is tailored. Audiences may also range from one person to hundreds of people. Briefings usually provide personal interface with those most in need of the intelligence presented--often generating better PIRs and additional IRs--but time constraints may preclude optimal preparation periods. Dissemination is tailored and often limited.

(2) **Documents.** Much intelligence is disseminated broadly via documents, which themselves may take many forms: plans, studies, analyses, estimates, assessments, reports, and electronic messages. Advantages include the ability to deal comprehensively, whether broadly or with a narrow focus, with complex subjects and those requiring broad dissemination; the ability to logically organize the intelligence in a manner conducive to user needs (e.g., basic summary up front, with detailed amplifying annexes and appendices as necessary); and their usability as a ready reference source, particularly during deliberate or contingency planning. The chief disadvantages are that these may quickly become obsolete, particularly once operations have commenced; they require a large commitment of time and other resources to develop; they lack immediate collector/producer/user personal interaction; and they are difficult to rapidly and broadly disseminate during tactical operations (whether hardcopy or electronic message documents).

Intelligence Estimates and Studies

Intelligence estimates and studies are normally written in peacetime or during the planning phase of potential operations. They are used to convey large amounts of background intelligence and other information to a wide audience when the need for such is not time-critical.

(3) **Electronic.** The first broadly available electronic formats were primarily technological modifications of traditional intelligence documents and graphical product formats. A very basic example is leveraging automated tactical local and wide area networks for coordinating intelligence requirements and disseminating intelligence throughout a MAGTF. More sophisticated examples include recently fielded and emerging specially designated intelligence systems, such as the Joint Deployable Intelligence Support System (JDISS) and the Intelligence Analysis System (IAS), which incorporate a broad variety of intelligence capabilities: transmission and managing of stated intelligence requirements; secondary imagery dissemination; multi-user access to common intelligence databases; and archiving and analytical exploitation of intelligence messages, files, target folders and other products. Additionally, improved near-real-time connectivity between intelligence collectors, producers and users highlights the principal advantage of electronic dissemination formats -- significantly greater

access throughout the MAGTF to organic and external intelligence capabilities.

(a) Reports

Reports

Intelligence reports and summaries are normally used to broadcast information electronically to a wide audience in order to update a current situation or subject of interest. Types can range from terrorist updates for travelers in peacetime to battlefield INTSUMS, INTREPs, and SALUTE reports. Normally released according to a predetermined time schedule, reports continuously "refresh" databases but may lag in timeliness during a fast-moving crisis or battle.

(b) Databases. Intelligence-related databases are major elements in MAGTF push/pull automated dissemination. The principal threat and environmental databases will be maintained within the intelligence battalion's Production and Analysis (P&A) Cell with the MEF CE. Additionally, subordinate units generally will establish and maintain their own databases, tailored to their units' intelligence needs. Major issues include user access, information updates, administration and maintenance responsibilities, their integration with other unit and pertinent external databases (e.g., operation, CSS), and available communication connectivity and capabilities.

(c) Sensor Data and Information Streams. The G/S-2, G/S-3 and G/S-6 must coordinate on information management and dissemination issues. This refers to the potential dissemination of intelligence information (e.g., UAV video footage) directly from a collector to a targeting or operational node (perhaps via an intelligence operations node). Both tactical advantages and risks must be considered.

(d) Common Operational Picture (COP) and Common Tactical Picture (CTP). Successful migration of current capabilities to facilitate a COP and CTP among units will improve operational interoperability, reliability and flexibility. For the near term, COP/CTP is still an evolving concept. A common operational database, which effectively combines visual and integration tools, is still needed: once configured and built, COP/CTP will become more real. The pace of technological and operating changes requires the following:

- Comprehensive intelligence individual and unit collective training in order to fully exploit these capabilities.
- Development of integrated and interoperable multi-force MAGTF, naval, and joint C4I doctrine and tactics, techniques and procedures (TTP).
- Multi-force exercise of these capabilities under realistic field operating conditions.

The MAGTF CE should be responsible for maintaining and disseminating the COP, which involves both friendly and enemy information. The MAGTF G/S-2 should receive inputs from

the MSCs via the IAS (SPOTREPs, etc.) analyze them, and produce and disseminate the enemy situation portion of the COP via the designated system(s) [Intelligence Operations Workstation (IOW), IAS, JDISS]. One major challenge is in determining the extent to which subordinate units need to/should control their own view of the battlefield. Additionally, data aggregation problems abound regarding a group picture. Other issues to be resolved include:

- Which different units should be designated “ground truth” disseminators for various sectors.
- How to accomplish COP/CTP track management. (Disseminating redundant tracks will quickly run the automated systems low on memory.)
- How to manage one COP database.
- How to pull a tailored picture from the MEF CE intelligence databases for use by subordinate units.
- Details on how to input intelligence information on the CTP in a visual format.
- Joint and multi-service intelligence standardization.

(4) Graphical Products. Examples include maps, overlays, annotated imagery, topographic products such as terrain models, simple graphics used to support intelligence briefs, and new and more sophisticated graphical capabilities and techniques that promise great improvement to combat readiness and operations. The chief benefit of graphical dissemination formats is that they may be assimilated and understood by people more quickly than textually-based formats. However, like with electronic dissemination formats, effective use of graphical product dissemination requires functional training, development of integrated multi-force standards and procedures, and realistic operational practice and evaluation of these. Additionally, while graphics may be useful for targeting and mission planning, textual grid coordinates are essential. Finally, graphics alone risk users assuming information that may not be accurate: thus, in most cases intelligence disseminated via graphics must be reinforced with supporting documents or other products.

Graphics

Graphics, such as those used in map enhancements or contained in annotated imagery, portray vast amounts of intelligence in a condensed form more easily interpreted by the human mind. When appropriate, they should be incorporated in all forms of intelligence production and dissemination.

1006. Overview of MAGTF Intelligence Dissemination Capabilities and Challenges

a. MAGTF CE Dissemination. The MEF’s intelligence battalion collection management/dissemination (CMD) section provides the core C2 for MEF intelligence dissemination operations by developing and coordinating the dissemination plan and reporting

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 criteria. The Surveillance and Reconnaissance Cell (SARC) executes reporting criteria. The
2 P&A Cell receives collected intelligence data and information, analyzes it, produces intelligence
3 products, and executes dissemination criteria. Key CIS resources required include IAS and JDISS,
4 with access to the full range of MAGTF communications [JWICS, SIPRNET, NIPRNET
5 (nonsecure), Defense Switched Network (DSN), etc.] for external dissemination; and IAS via
6 the tactical data network (TDN) and other MAGTF communications resources for internal
7 dissemination.

8
9 **b. Internal MAGTF Dissemination.** Within the MAGTF, especially for dissemination
10 between the CE and MSCs, the IAS, the IOW, and MAGTF TDN are the key tools for
11 electronic dissemination. IAS will be available at all command echelons down to the maneuver
12 battalion/squadron levels. Communications connectivity between the MAGTF CE and its MSE
13 HQs are predominantly provided by SATCOM, supplemented where practical with HF/UHF
14 radios, troposcatter multi-channel radio systems, telephone systems and couriers.

15
16 **c. External Dissemination.** The MAGTF CE will attempt to exploit all available external
17 capabilities (national, theater, JTF, etc.) to satisfy its IRs. Each dissemination supporting
18 database, specialized system, and team from the various intelligence agencies and DOD
19 organizations has specific connectivity and procedural requirements. These must be planned
20 for and coordinated extensively through the J-2 and J-6, or MARFOR headquarters (as
21 appropriate).

22
23 **d. MSC Level and Below.** Connectivity to the regiment/group level is principally via the
24 TDN, single-channel radio, various multichannel radio resources, telephones and couriers.
25 Finally, communications connectivity below the regiment/group level depends principally on
26 single channel radio primarily designed for voice traffic, with limited range and limited data
27 capacities (1.2 Kbps to 16 Kbps). Although these units possess tactical data systems, their
28 ability to exchange data traffic is limited due to the far less available bandwidth.

Chapter 2

Intelligence Dissemination Responsibilities

2001. General. Developing the capabilities and executing the operations to satisfy the wide variety of MAGTF intelligence dissemination requirements is an extremely difficult challenge that requires extensive planning, cooperation, coordination, flexibility, situational awareness, and perseverance. This chapter addresses the major dissemination roles and responsibilities of key operational and all-source intelligence personnel within the MAGTF.

2002. Commander. The commander is responsible for all intelligence and counterintelligence (CI) activities of the command. Although he may delegate specific authority to subordinates to assist in the performance of intelligence functions, the commander remains fully responsible for supervising all delegated activities. The commander controls the direction of intelligence by:

- Establishing intelligence priorities (PIRs) that serve as guideposts for intelligence dissemination activities.
- Identifying desired forms for dissemination.
- Establishing command and control and supporting CIS priorities and allocating resources accordingly.
- Monitoring and evaluating the overall effectiveness of intelligence dissemination operations.
- Ensuring the effective use of intelligence in unit planning and decision making.

2003. MEF Command Element G-2 Section and the Intelligence Battalion

a. Assistant Chief of Staff (AC/S), G-2. The AC/S G-2 has staff responsibility for intelligence and intelligence operations, to include intelligence dissemination. The commander relies on the intelligence officer to provide the necessary information on the weather, terrain, and enemy capabilities, status, and intentions. Through the intelligence operations plan and supporting intelligence and reconnaissance and surveillance plans, the AC/S G-2 plans and coordinates intelligence priorities; integrates collection, production and dissemination; allocates resources; assigns specific missions to subordinate elements; and supervises the overall intelligence and reconnaissance efforts. Specific dissemination responsibilities include:

- Developing and answering outstanding MEF and subordinate units' PIRs and IRs by planning, directing, integrating, and supervising organic multi-discipline MEF and supporting intelligence operations.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 • Preparing appropriate intelligence dissemination plans and orders for the MEF and
2 reviewing and coordinating the all-source intelligence dissemination plans of JTFs, theaters, and
3 other organizations.
4
- 5 • Submitting and coordinating all-source collection, production, and dissemination
6 requirements beyond the capability of the MEF to satisfy to higher headquarters for JTF, theater,
7 or national systems support.
8
- 9 • Ensuring intelligence information is rapidly processed, analyzed, and incorporated where
10 appropriate in all-source intelligence products, and rapidly disseminated to all MEF and external
11 units requiring these.
12
- 13 • Evaluating JTF, theater, and national intelligence dissemination support and coordinating
14 changes if necessary.
15
- 16 • Identifying and correcting deficiencies in intelligence and reconnaissance personnel and
17 equipment resources.
18
- 19 • Incorporating intelligence dissemination in training exercises in order to improve MEF
20 individual, collective, and unit readiness.
21
- 22 • Facilitating understanding of intelligence dissemination in support of the planning and
23 execution of MEF operations.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

b. G-2 Operations Officer. The G-2 operations officer, under the direction of the MEF AC/S G-2, has primary responsibility for intelligence support to the Commanding General (CG) and the remainder of the MEF CE in support of current operations and future operations. Specific dissemination-related duties include (see figure 2-1):

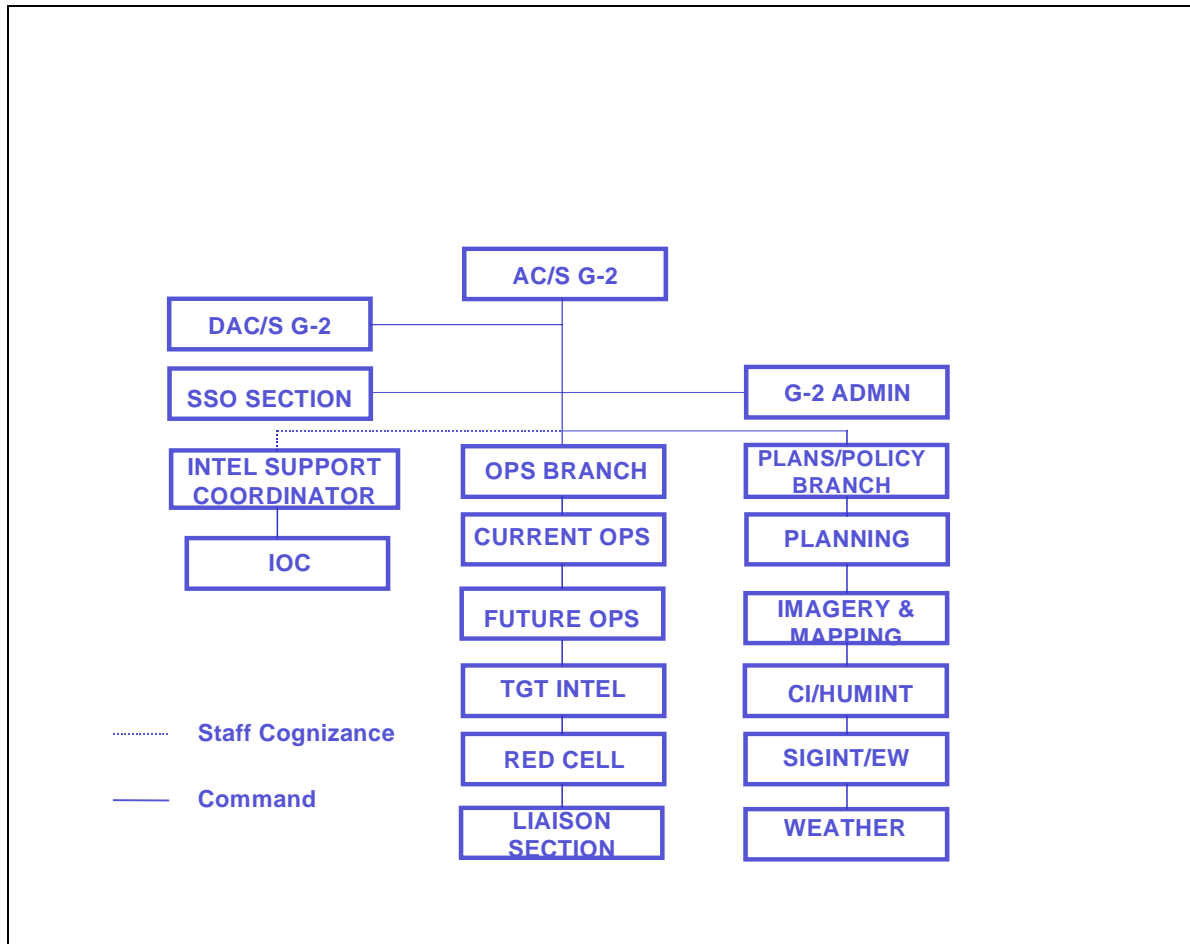


Figure 2-1. MEF G-2 Division Principal Staff Officers and Relationships

w Coordinating and providing intelligence support (to include dissemination support) to the CG, the G-3 operations section, and the rest of the MEF CE's battlestaff.

w Serving as the G-2 representative to the MEF CE crisis action team (CAT).

w Coordinating, providing, and supervising intelligence support to the MEF CE current operations center (COC), future operations center (FOC), and force fires.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

1
2 w Planning, directing and supervising the *Red Cell*.

3
4 w Providing recommendations on PIR and IR validation, prioritization, and taskings to
5 the AC/S G-2 and the Intelligence Support Coordinator (ISC).

6
7 w Coordinating and supervising the transition of intelligence planning and operations
8 from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current
9 operations, in order to effectively support the MEF's "single battle" transition process.

10
11 w Planning, directing and supervising MEF liaison teams to external commands and
12 intelligence organizations.

13
14 w Coordinating with the ISC and MEF MSCs' G-2 operations officers to ensure unity of
15 effort of MEF intelligence operations.

16
17 w Providing intelligence input and other support to MEF warning and fragmentary orders
18 and to operations related reporting (e.g., periodic situation reports).

19
20 w Coordinating intelligence training for the MEF G-2 section (to include dissemination
21 training) and providing G-2 oversight for and integration of the entire MEF intelligence training
22 program.

23
24 w Other intelligence support and tasks as directed by the AC/S G-2.

25
26 **c. G-2 Plans Officer.** The G-2 plans officer, under the direction of the MEF AC/S G-2, has
27 primary responsibility for intelligence support to the MEF CE's future plans cell. Specific
28 dissemination-related duties include (see figure 2-1):

29
30 w Planning the MEF concept of intelligence operations for approval by the AC/S G-2 and
31 subsequent implementation by the ISC based upon the mission, threat, commander's intent,
32 guidance, and concept of operations. This concept of intelligence operations will include a
33 supporting dissemination concept of operations.

34
35 w Leading, coordinating and providing intelligence support to the MEF G-5 future plans
36 section.

37
38 w Planning and coordinating intelligence support requirements for and the deployment of
39 intelligence elements and resources into the area of operations (AO).

40
41 w Providing recommendations on PIR and IR validation, prioritization, and taskings to
42 the AC/S G-2 and the ISC.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 w Coordinating, in conjunction with the ISC, G-2 development of Annex B (Intelligence)
2 and Annex M (Geospatial Information and Services) to MEF operations plan (OPLAN), their
3 supporting appendices, and all intelligence input to other annexes of OPLANs.

4
5 w Keeping the G-2 section, other CE staff sections, intelligence liaison personnel,
6 augmentees, and others as appropriate apprised of MEF intelligence dissemination actions and
7 requirements.

8
9 w Identifying requirements and providing recommendations to the G-2 operations officer
10 for MEF intelligence liaison teams to external commands (e.g., the JTF or other components'
11 headquarters) and intelligence agencies.

12
13 w Coordinating and developing policies for MEF intelligence, CI and reconnaissance
14 operations.

15
16 w Planning, directing and supervising the MEF G-2's imagery and mapping, CI/HUMINT,
17 SIGINT, and weather sections.

18
19 w Other intelligence support and tasks as directed by the AC/S G-2.

20
21 **d. Intelligence Battalion Commander/Intelligence Support Coordinator (ISC).** The
22 intelligence battalion commander is responsible for planning and directing, collecting,
23 processing, producing and disseminating intelligence, and providing CI support to the MEF,
24 MEF MSCs, subordinate MAGTFs, and other commands as directed.

25
26 w **Garrison.** In garrison the principal task of the intel bn commander is to organize, train
27 and equip detachments that support MAGTFs or other designated commands to execute
28 integrated collection, intelligence analysis, production and dissemination of intelligence
29 products. The composition of intel bn is shown in figure 2-2.

30
31

32
33 **Figure 2-2. Intelligence Battalion**
34

35 w **Actual Operations.** During operations the intel bn commander is dual-hatted as the
36 ISC¹, serving as such under the direct staff cognizance of the MEF AC/S G-2. The intel bn's S-3
37 section along with the operations center element of the MEF G-2 form the core of the ISC

¹ During garrison operations, most of the tasks listed here are the responsibility of the G-2 operations officer.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

support effort, with planning, direction, and C2 conducted within the intelligence operations center's (IOC's) support cell. As the ISC he is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF all-source intelligence, CI, and reconnaissance operations. Specific dissemination-related responsibilities of the ISC during actual operations include:

- Implementing the concept of intelligence operations (and the supporting dissemination concept of operations) developed by the G-2 plans officer and approved by the AC/S G-2.

- Establishing and supervising operation of the MEF IOC, which includes the support cell, the SARC, and the P&A cell (see figure 2-3.) Generally the IOC will be co-located with the MEF CE's main command post.

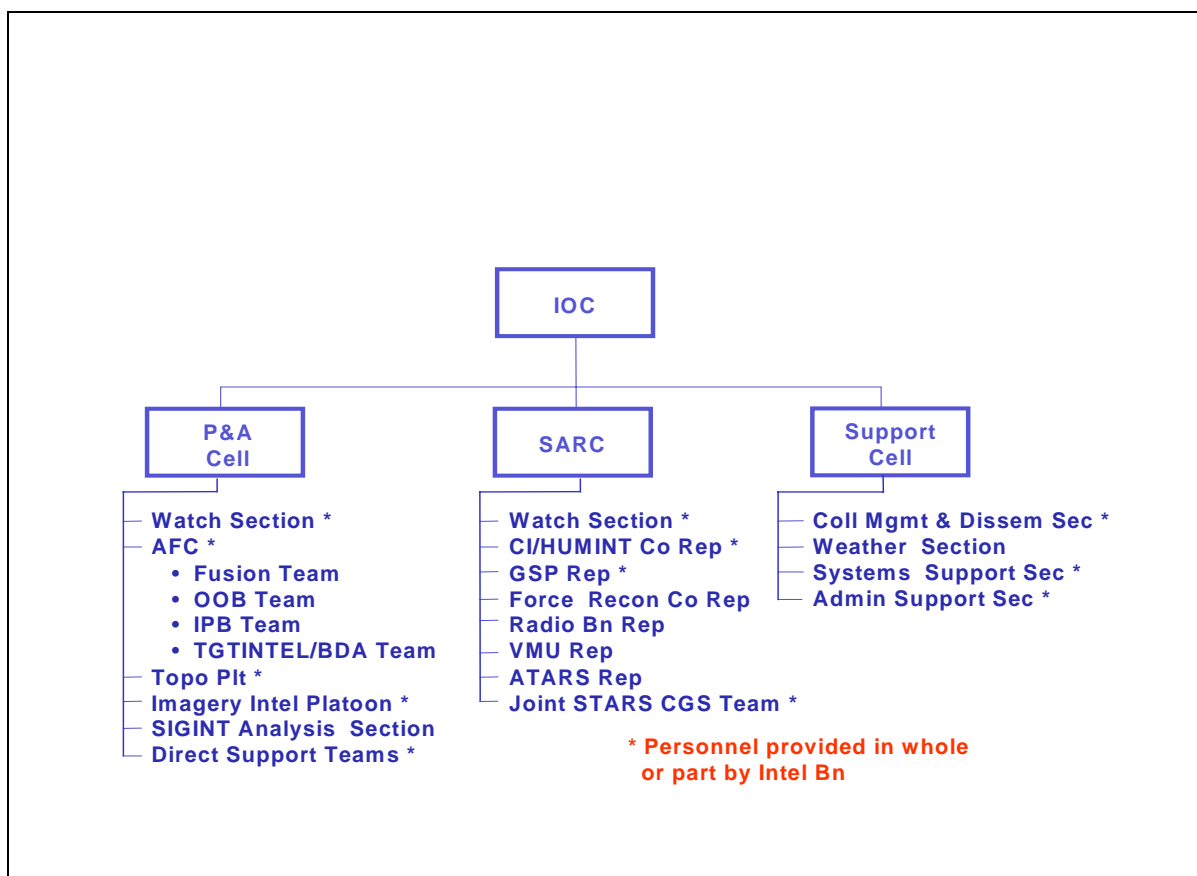


Figure 2-3. Intelligence Operations Center

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1
2 x Developing, consolidating, validating, and prioritizing² recommended PIRs and IRs
3 to support MAGTF planning and operations.

4
5 x Planning, developing, integrating, and coordinating MEF intelligence collection,
6 production, and dissemination plans.

7
8 x Performing staff cognizance of and the effective organic and external integration and
9 employment of MEF imagery intelligence (IMINT), signals intelligence (SIGINT),
10 counterintelligence (CI), human resources intelligence (HUMINT), geographic intelligence
11 (GEOINT), ground remote sensors, ground reconnaissance, and tactical air reconnaissance
12 intelligence collections, production, *and dissemination operations*.

13
14 x Developing, in conjunction with the G-2 plans officer and G-2 operations officer, and
15 completing Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF
16 operations orders (OPORD), their supporting appendices, and all intelligence input to other
17 annexes of OPORDs.

18
19 x Planning, developing, integrating, and coordinating intelligence and CI support to the
20 commander's estimate, situation development, indications and warning, force protection,
21 targeting, and combat assessment.

22
23 x Managing and fusing the threat (or *red*) COP/CTP inputs from subordinate units and
24 external commands and intelligence agencies into the MEF CE's threat COP/CTP.

25
26 x Providing intelligence support to the MEF CE G-2 section and the MSCs.

27
28 x Preparing the intelligence and CI estimates to support G-2 plans.

29
30 x Planning, developing, and coordinating the intelligence dissemination CIS
31 architecture, to include its integration with and support of intelligence and reconnaissance
32 requirements.

33
34 x Coordinating and integrating MEF intelligence dissemination operations with other
35 service components, the JTF joint intelligence support element (JISE), the theater joint
36 intelligence center (JIC) or joint analysis center (JAC), and national intelligence agencies and, to
37 include all aspects of intelligence reachback support.

38

² The ISC is tasked to perform PIR and IR validation and prioritization *only* during actual operations when the IOC is activated. During routine peacetime operations the PIR/IR validation and prioritization tasks are the responsibility of the MEF CE's G-2 operations officer.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

x Assisting with the evaluation and improvement of MEF intelligence dissemination operations.

x Other intelligence support and tasks as directed by the AC/S G-2.

(See figure 2-4 for a summary of the principal responsibilities of the AC/S, G-2's, three principal subordinate staff officers.)



Figure 2-4. AC/S G-2's Principal Subordinate Staff Officers and their Responsibilities

e. Collection Management/Dissemination Officer (CMDO). The CMDO is sourced from the intel bn's S-3 section and is subordinate to the intel bn commander/ISC during operations. The CMDO is responsible for formulating detailed intelligence collection requirements (ICRs) and ***intelligence dissemination requirements (IDRs)*** and tasking and coordinating internal and external operations to satisfy these. The CMDO receives validated PIRs and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans. The CMDO is also responsible for validating and forwarding MEF and MSC requests for national and theater collection and dissemination support using appropriate intelligence tools and TTP. He also is responsible for coordinating intelligence CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations. During operations the CMDO works within the support cell (see figure 2-3). In coordination with the P&A cell OIC, the SARC OIC, G-2 operations officer, intelligence unit COs/OICs, and the MEF G-6, the CMDO is responsible to the ISC for the following dissemination-related tasks:

w Determination and coordination of the collection and dissemination efforts of PIRs/IRs.

w Determination of PIRs/IRs and preparation of requests for intelligence (RFI) that are beyond organic capabilities and preparing submissions to higher headquarters and external intelligence agencies for support.

w Recommending dissemination priorities, development of intelligence reporting criteria, and advising on and selecting dissemination means.

w Developing and coordinating intelligence collection plans, coordinating and integrating these with MEF, other components, JTF, theater, and national intelligence production operations.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 w Developing and coordinating intelligence dissemination plans and supporting
2 architectures for both voice and data networked communications, and coordinating and
3 integrating these with MEF, other components, JTF, theater, and national intelligence CIS and
4 dissemination operations.

5
6 w Monitoring the flow of intelligence throughout the MAGTF and ensuring that it is
7 delivered to intended recipients in a timely fashion, is understood, satisfactorily meets their
8 needs, and whether any new IRs result.

9
10 w Troubleshooting dissemination problems: identifying intelligence dissemination
11 problems, recommending solutions, and ensuring timely corrective actions are initiated and
12 completed.

13
14 w Evaluating the effectiveness of MEF and supporting IMINT collection and
15 dissemination operations.

16
17 **f. Surveillance and Reconnaissance Cell (SARC) OIC.** The SARC OIC is also an immediate
18 subordinate of the ISC and is responsible for supervising the execution of the integrated organic,
19 attached, and direct support intelligence collection and reconnaissance operations (see figure 2-
20 3). The SARC OIC is responsible to the ISC for accomplishing the following:

21
22 x Coordinating, monitoring, and maintaining the status of all ongoing intelligence
23 collection operations. This includes:

24
25 x Missions, tasked ICRs, and current reporting criteria for all collection missions.

26
27 x Locations and times for all pertinent fire support control measures.

28
29 x Primary and alternate CIS plans for both routine and time-sensitive requirements,
30 both for intelligence collectors as well as between the collectors or the SARC and key MEF CE
31 and MSC C2 nodes, in order to support ongoing C2 of collection operations and dissemination of
32 acquired data and intelligence to those needing it via the most expeditious means.

33
34 w Conducting detailed intelligence collection planning and coordination with the MSCs
35 and intelligence organizations planners, with emphasis on ensuring understanding of the
36 collection plan and specified intelligence reporting criteria.

37
38 w Ensuring other MAGTF C2 nodes (e.g., the current operations center, force fires center,
39 etc.) are apprised of ongoing intelligence and reconnaissance operations.

40
41 w Receiving routine and time-sensitive intelligence reports from deployed collection
42 elements; cross-cueing among intelligence collectors, as appropriate; and then rapidly

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

disseminating reports to MAGTF C2 nodes and others in accordance with standing PIRs/IRs, intelligence reporting criteria and dissemination plans, and the current tactical situation.

g. Production and Analysis (P&A) Cell OIC. The P&A cell OIC is the third principal subordinate to the ISC, with primary responsibility for managing and supervising the MEF's all-source intelligence processing, analysis and production efforts (see figure 2-3). Key dissemination-related responsibilities include:

- w Planning, directing and managing operations of the all-source fusion platoon (to include the fusion, order of battle, intelligence preparation of the battlespace (IPB), and target intelligence/BDA teams), the topographic platoon, the imagery intelligence platoon (IIP), the direct support teams (DST), and other analysis and production elements as directed.

- w Coordinating and integrating P&A cell operations, estimates, and products with the MEF G-2 section's G-2 operations branch and its *Red Cell* operations and intelligence estimates.

- w Maintaining all-source automated intelligence databases, files, workbooks, country studies and other intelligence studies.

- w Planning and maintaining imagery, mapping and topographic resources and other intelligence references.

- w Administering, integrating, operating, and maintaining intelligence processing and production systems, both unclassified general service (GENSER) and SCI information systems (e.g., the image product library [IPL], JDISS, IAS).

- w Conducting analysis and preparing all-source intelligence estimates, reports and other products, briefings, etc.

- w Supervising and performing the sanitization of sensitive compartmented information (SCI) and its subsequent dissemination.

- w Analyzing, fusing, and tailoring all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.

- w Developing and maintaining current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.

- w Managing and fusing the threat (or *red*) COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.

- w Disseminating intelligence reports and other products throughout the MEF and to

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

external organizations in accordance with the dissemination plan and current reporting criteria.

h. The Intelligence Watch Officer (IWO), Current Operations Center (COC). The COC IWO is responsible for implementing intelligence operations in the COC and thus is the focal point for all current intelligence and CI matters. Key tasks include: maintaining situational awareness of the current threat and the environment; monitoring ongoing intelligence, operations, CIS and other MAGTF activities; initiating intelligence actions as required; and monitoring the MAGTF-wide status of standing PIRs. The COC IWO has principal responsibility for:

- Providing intelligence support to G-3 current and future operations centers, force fires center, G-6 systems control, and other CE elements as appropriate.

- Continuous coordination with subordinate units' intelligence officers, JTF JISE watch officer, and other current intelligence watch elements in order to identify IRs and to provide intelligence support, as appropriate.

- Disseminating intelligence meeting alarm reporting criteria.

- Keeping other elements of the intelligence section and IOC aware of current tactical developments that require changes in previously established intelligence priorities or planned tactical and intelligence operations.

- Disseminating specified intelligence products (e.g., periodic intelligence summaries, COC briefings, current intelligence reports).

- Acting as net control for the MEF intelligence net (when established).

i. Special Security Officer (SSO). The SSO has primary responsibility for managing the MEF's sensitive compartmented information (SCI) program; planning and supervision of SCI communications; and the security, control and use of SCI materials, equipment and products. The SSO's dissemination responsibilities arise from the special security requirements of SCI. Prior to operations, he assists the intelligence dissemination effort by:

- Identifying SCI products for the MEF CE and all subordinate units.

- Assisting with identifying and acquiring mission unique SCI products in support of MEF requirements.

- Planning and coordinating MEF SCI CIS architecture integrated with joint, theater and national systems.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 • Identifying requirements for and planning and supervising SCI courier, electronic, and other
2 CIS in support of garrison and contingency planning needs.

3
4 • Supervising the security of SCI sanitization efforts critical to the rapid and secure
5 dissemination of time-sensitive intelligence to MEF elements lacking SCI access.

6
7 • Administering the SCI access program to ensure that all MEF personnel requiring regular
8 or time-sensitive SCI access have satisfied necessary personnel security requirements.

9
10 • Establishing and ensuring the security of the MEF CE SCI facility and all SCI resources
11 within it.

12
13 **2004. Other Command Element Staff**

14
15 **a. G-1**

16
17 • **Personnel Requirements.** The G-1 is responsible for all personnel requirements with regard
18 to the intelligence effort. MEF intelligence dissemination operations may require personnel
19 augmentation to satisfy all requirements, particularly to staff key contingency billets with the
20 G-2 section and intelligence battalion. All such requests for intelligence personnel
21 augmentation will be developed by the MEF G-2 and provided to the G-1 for either internal
22 sourcing or for forwarding to higher headquarters for action (e.g., global sourcing).

23
24 • **Courier Requirements.** Additionally, the G-1 is responsible for the establishment,
25 operation, and supervision of physical courier support.

26
27
28
29
30 **b. G-3**

31
32 • **Tactical Employment of Units.** The G-3 is responsible for planning, coordinating, and
33 supervising the tactical employment of units. As such, the movement and operations of
34 intelligence and supporting units must be coordinated by the G-2 with the G-3 for integration
35 in future and current operations planning.

36
37 • **Key Recipient of Intelligence.** Additionally, since the G-3 has primary responsibility for the
38 planning and operations of maneuver and fires, he is a primary user of various forms of
39 intelligence and sensor information. *The G-2 and G-3 must coordinate closely to ensure*
40 *dissemination meets MEF operational and tactical needs.*

41
42 **c. G-4**
43

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

- 1 • **External Assets Requirements.** The G-4 is responsible for the logistic support of the MEF,
2 which may include dissemination-related assets from national, theater, joint, other-service, or
3 allied sources. To ensure the required support is available, arrangements should be
4 developed early in the deployment which meet the particular needs of the deployed supported
5 unit.
6
- 7 • **Maps and Charts.** Additionally, the G-4 is responsible for all MEF supply support, to
8 include the distribution of maps and charts.
9
- 10 **d. G-5.** The G-5 is responsible for all long-range (future) and joint planning matters. Normally,
11 a G-5 is found only at the MEF and MARFOR levels; at lower MAGTF echelons future planning
12 is the responsibility of the G-3. The G-5 needs to understand intelligence dissemination and the
13 overall intelligence concept of operations, unique requirements, and other type of support
14 required for intelligence operations.
15
- 16 **e. G-6.** The G-6 is responsible for CIS support to intelligence, including dissemination. The G-
17 6 is responsible for providing for and protecting CIS connectivity and operations, both within and
18 external to the MEF. This includes providing the communication paths, network accesses, radio
19 nets and frequencies, telephone and other communication support to MEF intelligence, CI and
20 reconnaissance operations. This requires extensive systems knowledge across the spectrum of
21 intelligence CIS. ***Intelligence CMDO, plans and operations personnel must coordinate***
22 ***extensively and continually with the G-6.***
23
- 24 **2005. MEF Major Subordinate Commands (MSC) Intelligence Officers.** All MSC
25 intelligence officers are responsible for effectively using their intelligence and CIS resources for
26 appropriate intelligence dissemination with higher, adjacent, supporting, and subordinate
27 elements. Key tasks of MSC intelligence officers include:
28
 - 29 • Planning and implementing a concept for intelligence support based on the mission,
30 concept of operations, and commander's intent.
31
 - 32 • Providing centralized direction of and support to command intelligence operations, to
33 include intelligence elements attached to or placed in direct support of the unit.
34
 - 35 • Consolidating, validating, and prioritizing unit IRs and dissemination needs.
36
 - 37 • Submitting consolidated requests for external intelligence support to the MEF CE.
38
 - 39 • Coordinating CIS links to pertinent supporting external intelligence collection,
40 production, and dissemination elements and operations.
41

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 • Providing timely, accurate feedback on the level of unit satisfaction regarding intelligence
2 dissemination support received.
- 3
- 4 • Providing intelligence support to unit current and future operations and all C2 centers.
- 5
- 6 • Analyzing and preparing intelligence products, estimates and reports.
- 7
- 8 • Providing intelligence briefings to support unit operations.
- 9
- 10 • Identifying problems and initiating corrective actions/solutions for unit intelligence, CI
11 and reconnaissance operations.
- 12
- 13
- 14
- 15
- 16

Chapter 3

Intelligence Dissemination Methodology

3001. Overview. Effective dissemination operations will only result if dissemination planning begins and is continually coordinated with development of the intelligence, operations, and CIS operational concepts and supporting intelligence collection and production plans. The line of departure for Corps-wide success begins with a common understanding of a simple dissemination methodology. Each intelligence requirement has three parts -- an intelligence collection requirement (ICR), an intelligence production requirement (IPR), and an intelligence dissemination requirement (IDR). Each dissemination requirement should be processed individually, using the methodology described below. Figure 3-1 depicts the steps in MAGTF intelligence dissemination methodology.

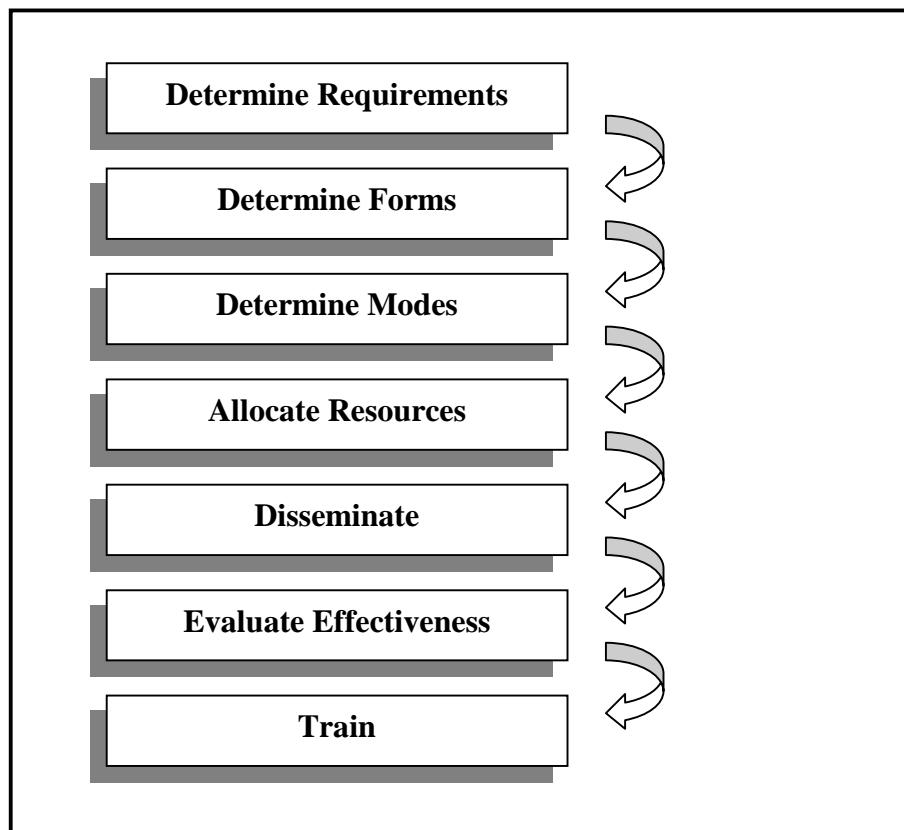


Figure 3-1. Dissemination Methodology

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

3002. Determine Dissemination Requirements:

**Identify what intelligence is needed, who needs it, where they are,
when it is required, and assign priority.**

- a. **In the broad sense:** Commanders determine what intelligence is needed and when it must be available; intelligence personnel develop and implement the flow of intelligence.
- b. **From the intelligence dissemination perspective, there are several things to keep in mind:**
- **Think optimum utilization.** It is critical that G/S-2 staffs exercise caution and review carefully when a request for intelligence is received. To preclude wasting precious time on unnecessary or lower priority tasks, intelligence personnel should determine exactly what intelligence is needed, who needs it, when is it needed, and where it needs to be sent for optimum utilization.
 - **Stay in contact with commanders and other intelligence requestors.** Because all dissemination variables are subject to change--especially in a tactical environment--it is important that intelligence disseminators remain in frequent contact with the requestor in order to maintain timely and complete understanding of their IRs and thus minimizing intelligence operations changes and distribution delays.
 - **Determine common intelligence requirements.** In conjunction with the MAGTF staff and subordinate commands' intelligence officers, the G/S-2 staff should determine what the common IRs are. The idea is to minimize human intervention in passing data, and design/model the CIS architecture and dissemination concept of operations, whenever possible, to allow users who routinely need certain kinds of information and intelligence to get it themselves. For example, if the G/S-4 has access to SIPRNET (as well as trained/cleared personnel), he can pull routinely needed intelligence from a database (e.g., on port characteristics) without having to compete for G/S-2 support. This is where "standing IRs" and supporting ICRs, IPRs, and IDRs come into play: design the information blueprint around standing IRs, then design the applications and architecture to support it.
 - **Develop Planning Tools.** Use PIRs and IRs to guide dissemination requirements; develop collector reporting and intelligence dissemination flow diagrams and planning matrices (discussed in Chapter 4). Good reporting and dissemination flow diagrams and matrices assist in dissemination development, planning and execution. They also provide COC, P&A Cell, and SARC watch personnel with references to guide them in problem management and solving, and articulating dissemination decisions.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

c. During garrison operations, dissemination requirements determinations focus on:

1. Identifying operations and contingency plans (CONPLANS) that the MAGTF may be committed to.
2. Identifying and refining PIRs and IRs for each CONPLAN and OPLAN, and then specifying and interpreting associated ICRs, IPRs, and IDRs.
3. Establishing accessibility of a supporting all-source intelligence reference library, files, databases and other intelligence support materials (e.g., imagery, geospatial, and associated intelligence products), ensuring composition is known to all MAGTF intelligence personnel, key intelligence users, and commanders.
4. Identifying supporting intelligence community databases exploitable via automated intelligence systems and networks, to include necessary user identifications (userid), passwords, and special considerations.
5. Coordinating development of unit-tailored and MAGTF-integrated statements of intelligence interest based upon the above requirements determinations.
6. Identifying intelligence address indicator groups (AIGs), DSSCS address groups (DAGs), and other electronic message addresses and groupings, common address designators (CADs) and other recurring or periodic electrical products disseminated by intelligence organizations pertinent to MAGTF's PIRs, IRs, and other areas of interest (AOI) and responsibility (AOR).
7. Using the above information to identify or refine -- by OPLAN/CONPLAN or potential contingency -- current known intelligence gaps based upon specified or most likely contingencies and missions.
8. Refining MAGTF dissemination routine and time-sensitive requirements identification SOPs, to include integration with other functional SOPs and across all command echelons.
9. Designing or modifying CIS architectures to include: organic intelligence and reconnaissance units, MEF-wide, afloat, joint or combined, and possible civil-military variations.
10. Regular and realistic training of all intelligence personnel to improve their understanding and operational capabilities.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1 11. Regular and realistic training of commanders, operations, CSS, CIS and other
2 personnel --particularly those serving as watch personnel in COCs/FOCs,
3 FSCs/FFCs/SACCs, TACLOG, SYSCONs and TECHCONs, etc.
4

5 **d. In response to developing crisis situations, receipt of an alert or warning order, or an**
6 **actual operational commitment, dissemination requirements determinations focus on:**
7

- 8 1. Disseminating throughout the MAGTF the most current available intelligence and CI
9 estimates pertinent to the mission, situation, and AO.
10
- 11 2. Identifying and prioritizing PIRs, IRs, and supporting ICRs, IPRs, and IDRs, with
12 emphasis on immediate mission analysis and planning needs.
13
- 14 3. Identifying and operational checking--or implementing—CIS capabilities throughout
15 the MAGTF and with key external commands and intelligence elements.
16
- 17 4. Identifying, organizing and reviewing on-hand intelligence materials pertinent to the
18 situation, ensuring composition and availability is known to all intelligence personnel
19 and pertinent commanders and planners.
20
- 21 5. Identifying unique electronic messages, specialized databases and other intelligence
22 products, JWICs and SIPRNET homepages, and the initial production and
23 dissemination plans initiated by higher headquarters and supporting intelligence
24 organizations (that are specifically focused upon the developing situation or mission);
25 ensuring userid, passwords, etc. are obtained for all requiring access throughout the
26 MAGTF.
27
- 28 6. Based upon initial higher headquarters' direction, MAGTF mission analysis, and
29 commander's (to include subordinate units) intent, revising initial PIRs, other IRs and
30 identifying associated LTIOV, who (MAGTF Commander, staff planners, subordinate
31 units) requires answers to each and their current location, and priorities.
32
- 33 7. In coordination with production planners, identifying type products, formats, and
34 primary and alternate dissemination means for priority intelligence products.
35
- 36 8. In coordination with production planners and the special security office (SSO),
37 determining proper authority/sanitization and other special access requirements and
38 authorities.
39
- 40 9. Reviewing MAGTF plan for periodic review and currency assessments of identified
41 PIRs/IRs, to include procedures for periodically updating subordinate units on the
42 status of these.
43

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

10. Updating accurate intelligence AIGs, electronic message addresses and groupings, and CADs for dissemination operations.

11. Identifying, prioritizing, and initiating action for all dissemination deficiencies and immediate challenges (e.g., releasability to coalition forces).

3003. Determine Dissemination Form:

Identify the form that best meets the user's needs.

a. Considerations. Intelligence is disseminated in various forms (see Figure 3-2), depending on user needs, the amount of intelligence to be transmitted, timeliness requirements, and the quantity and echelons of the recipients. **The following must be considered:**

- **Best Form.** The best form(s) for dissemination is the one that best meets the needs of the user. It must answer the user's needs in the timeliest manner consistent with the urgency of the tactical situation. If the user is unsure of exact needs, a mutual understanding between the recipient and the producer usually results in a serviceable product.
- **Formatting Considerations.** Disseminators must be able to prepare and transmit the formatted intelligence in time to satisfy the user's LTIOVs or it is of little value. ***A well designed dissemination plan will take formatting factors into account and save manhours otherwise spent on re-drafting and copying.*** After selecting a pathway, disseminators must coordinate with producers to ensure the format of the intelligence product meets the needs of the mode of transmission. For certain recipients, such as at the MEF and JTF levels, graphical materials are often appropriate and desired. Graphics alone, however, will not suffice for targeting and mission planning needs. Further, during combat operations graphics typically do not work well at the regiment/MAG levels and below; with the result that most dissemination at these levels remains secure voice radio or telephone.
- **CIS Capabilities.** It is important to consider user's CIS capabilities. For example, the disseminator may initially plan to send most products via electronic message but, after taking into account that many of the intended recipients are in a highly mobile situation and thus have only point-to-point phone/radio communications, will employ alternate CIS means. Consequently, dissemination planners and managers must know the CIS capabilities – and current status – of all supported elements, to include those two or more echelons lower.

FORMS AND PATHWAYS FOR DISSEMINATING INTELLIGENCE

VERBAL

HARDCOPY

SOFTCOPY

GRAPHICS

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

Figure 3-2. Forms and Pathways for Disseminating Intelligence

b. During garrison operations, dissemination forms determinations focus on:

1. User's IRs, desires, and timeliness requirements.
2. Assessing all MAGTF units and supporting intelligence production agencies personnel and technical capabilities to prepare and transmit all possible intelligence product formats (to include extensive CIS training).
3. Analyzing previous exercises and operational lessons learned to identify the most effective preferred and primary alternate dissemination forms. The goal is to specify -- by mission and principal tasks, cross-referenced by type MAGTF unit and/or staff section -- which dissemination forms generally best satisfy their intelligence needs. The product of this effort is format determination criteria that must be incorporated into MAGTF standing dissemination TTP. Additionally, this will further develop disseminators' tactical and technical knowledge and expertise, allowing for greater and more effective intuitive decision making during high tempo operations or unusual situations.
4. Determining planning estimates of the time needed to prepare and transmit each type intelligence product format to typical ultimate users.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

5. Regular and realistic training of all intelligence personnel to improve their understanding and operational capabilities.

c. In response to developing crisis situations, receipt of an alert or warning order, or an actual operational commitment, dissemination forms determinations focus on:

1. Verifying planning timelines and each user's intelligence needs and associated LTIOV.
2. Maintaining awareness of MAGTF CIS architecture installation, operations and changes, as well as courier plans and capabilities.
3. Prioritizing and effectively managing intelligence processing, production and communication resources.
4. Using established format determination criteria and the above information, selecting formats that best satisfy user requirements.
5. Rapidly modifying SOPs consistent with METT-T and ensuring all are aware of any changes.

3004. Determine Dissemination Mode

Identify Dissemination Channels and Capabilities:

- Identify and select both routine and time-sensitive modes.
- Determine and prioritize both dissemination point-to-point and broadcast modes for the widest possible range of tactical situations, to include both standard and alarm situations and criteria.
- Maintain awareness of the status of all MAGTF and key external CIS plans and operations.

a. General. Intelligence can be conveyed by various means, depending primarily on the nature and urgency of the intelligence, the tactical situation and the pathway available. Both broadcast and point-to-point (including multiple echelons down) modes must be planned in detail. ***MAGTF intelligence staffs--through coordination with communications personnel--should plan for several dedicated pathways for intelligence dissemination as well as for primary and alternate dissemination via common pathways.*** As always, it is important to economize on available CIS bandwidth. Potential ways to distribute intelligence are depicted in figure 3-2.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

b. During garrison operations, dissemination channels identification focuses on:

1. Assessing, in coordination with the MAGTF G-3 and G-6, MAGTF internal and external standing CIS capabilities, architectures, SOPs and TTP.
2. Overlaying and analyzing (by mission, principal tasks and the six intelligence functions) for designated OPLANS or contingencies, the standing CIS architecture and most likely MAGTF task-organization to be employed for each. The intelligence planning focus is to determine availability and value of broadcast and point-to-point modes and pipeline and alarm channels across the spectrum of military operations. Critical information to determine includes type CIS pathways (e.g., secure telephone, single/multichannel radio, local and wide area networks, couriers, record communications, VTC), and for each, the network composition (i.e., which units/organizations are standing or as required net members), transmission capacity, physical entry/exit points, operating/accessing procedures, installation and restoration priorities.
3. Doing same for intelligence units' internal intelligence C2 and dissemination. This includes: from collector back to its principal CIC/IOC operational node; from collectors to other echelons' HQ (e.g., from force recon team to an infantry regimental HQ); and for integrated, cross collector operations (e.g., between a RadBn RRT and force recon teams).
4. Analyzing intelligence data and operational planning information flows within the G-2, and to other commands and sections (to include those of subordinate units) to establish dissemination procedures and identify potential problem areas.
5. Integrating the information into the standing intelligence concept of operation for each type mission and standing OPLANS/CONPLANS. The end product is a detailed intelligence dissemination concept and supporting architecture and TTP for each type mission (or, for standing OPLANS/CONPLANS, the actual dissemination contingency plan).
6. Identifying personnel and equipment deficiencies and then developing, planning and monitoring corrective or contingency actions.
7. Regular and realistic training of intelligence personnel and users to improve their understanding and operational capabilities.
8. Ensuring commanders, operations, CIS and other key non-intelligence personnel have on-line access and individual skills and abilities to "pull" intelligence from databases, www sites and other sources.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

c. In response to developing crisis situations, receipt of an alert or warning order, or an actual operational commitment, dissemination channels identifications focus on:

1. Rapidly assessing, in coordination with the MAGTF G-3 and G-6, MAGTF internal and external CIS capabilities, architectures and TTP.
2. Identifying and implementing required changes to these, and communicating and coordinating same with all concerned MAGTF units.
3. Integrating same as required with the CIS architectures and intelligence concepts of operations of the JTF headquarters, other services, allied, multinational and supporting intelligence organizations.
4. Verifying the reliability of MAGTF-wide dissemination primary and alternate channels -- with emphasis on C2 of intelligence and reconnaissance units and time-sensitive and alarm channels -- initiating as necessary corrective actions and alternate paths.
5. Immediately identifying/validating personnel and equipment deficiencies and unique needs, and then initiating required corrective action (e.g., global sourcing, changes to dissemination plans, etc.).
6. Ensuring globally sourced MAGTF units and personnel are quickly trained regarding dissemination activities pertinent to their efforts.

3005. Allocate Resources. There will always be more requirements and employment possibilities than available intelligence organizational, personnel, and equipment resources and capabilities. **Task organization of intelligence support units, resources and capabilities is one of the principal ways for commanders to shape the intelligence effort.**

Regarding dissemination, the unique and greater capabilities of some intelligence units and resources can significantly enhance the ability of supported G/S-2 sections to access, develop and use timely, mission-focused intelligence. Most all intelligence, reconnaissance and CI units are task-organized to provide specific intelligence capabilities, as influenced by METT-T and the commander's guidance – in particular, the threat situation and capabilities, the supported unit's anticipated IRs (as determined through planning and IPB), the concept of operations, and the concept of intelligence support.

It is critical for the commander and intelligence officer exercising centralized control to allocate

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

resources to ensure that the needs of subordinate commanders – particularly those crucial to mission accomplishment – are properly addressed and supported. Detachments from one or more intelligence/reconnaissance/CI units may be placed in direct support (DS) or attached to subordinate units; or they may be used to create enhanced intelligence nodes in support of a subordinate unit or center (e.g., the rear area operations center; civil-military operations center). This must be done with the G/S-3 (for unit concept of operations and tactical task organization), the G/S-6 (for CIS resources), the G/S-1 (for personnel augmentation and courier support), the G/S-4 (for unique intelligence elements' CSS support) and within the G/S-2 section for effective management of dissemination personnel and assets.

Considerations When Allocating Dissemination Resources

- **Concept of Operations and Tempo.** The overall concept of operations (especially the designation of main and priority supporting efforts and the need for any specialized, non-routine intelligence node), the intelligence concept of support, and the nature of the PIRs and IRs (especially that of the threat and other key intelligence targets – e.g., those tactical units using low power radios) are key considerations.
- **Tactical Equipment.** The ability of a unit to integrate, plan and direct, and support (both CIS and CSS) attached or direct support intelligence elements. Regular, realistic tactical training during peacetime is the principal test of this readiness.
- **Technical Capabilities.** While significant, the MAGTF CIS architecture is optimized for certain task organizations and operating methodologies. Intelligence resource planners must comprehensively understand the unique strengths and weaknesses of the CIS architecture at all command echelons, as well as how those are affected when intelligence elements are attached to or placed DS to subordinate elements. For example, both single-channel voice and multi-channel data communications connectivity, operational capabilities and system administrative requirements may increase dramatically if a large number of intelligence elements must be integrated into a unit's main command echelon (typical at all GCE echelons). The supported unit's commander, operations officer and CIS officer must also thoroughly understand the effects of such intelligence task organization.
- **C2 Effects.** Even when intelligence elements are attached or placed DS to subordinate units, in most cases the MAGTF commander retains technical control of their operations, which he exercises via the G/S-2. This must be thoroughly understood and evaluated by commanders and operations officers as it directly affects their C2 authorities over, as well as the CIS support they must provide to, these intelligence elements.

3006. Disseminate the Intelligence and Take Subsequent Action. As already stated, intelligence has no value until it has been provided to commanders and other users in time to support operations. Once prepared, an intelligence product must be disseminated as quickly as possible for use by all users. Dissemination planners should always anticipate clogged or disabled communication links by

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

planning alternate distribution means. Redundancy must be planned for and used as needed. *Lead and manage the dissemination effort: apply “immediate action” dissemination remedies as needed.*

Considerations During Dissemination

- **Current Tactical Situation.** The dissemination plan will provide guidance for when, to whom, and how to disseminate the various types of intelligence and products. Regarding time-sensitive intelligence and answers to most PIRs, disseminators must always further evaluate the intelligence against the current tactical situation and ask who in addition to planned recipients has a need for the intelligence, and then initiate necessary action.
- **Status of Current CIS Readiness.** The principal dissemination mode or channel maybe degraded or inoperable when needed – to include those used by intended recipients. Accordingly, dissemination managers must continuously know the status of all CIS resources and pathways – primaries and alternates – in order to immediately initiate and direct dissemination operations. Continuous coordination with the G/S-2 COC watch officer and the G/S-6’s systems control (SYSCON) and technical control (TECHCON) centers is mandatory in order to rapidly know when problems are being experienced and what alternate means are available to meet immediate intelligence operations needs.
- **Leadership and Quality Control of Dissemination.** Dissemination planning is predominantly centrally-managed. Dissemination execution, however, is decentralized and will be conducted by a wide variety of individuals – P&A Cell, SARC, and COC intelligence personnel; intelligence, CI and reconnaissance collectors; and even operations, fires and other non-intelligence personnel. Additionally, with the fielding and greater employment of new CIS technologies and the implementation of newer operational concepts and functional methodologies, far greater intelligence access and intelligence dissemination are now possible from commands and organizations external to the force (and vice versa) to command echelons throughout the MAGTF. Together with the ability of all to pull information from non-military or intelligence sources – news media, academia, NGOs – and use it as (or in lieu of) intelligence is a major leadership and quality control challenge. Risks include incorrect, misleading, dated or incomplete data; excessive data; and “conclusive” data without seeing or understanding what it is based upon. Even for dissemination within the MAGTF, the many probable disseminators will intensify intelligence leaders’ efforts to ensure all needing it have in fact received it, whether it is understood, the degree to which it has satisfied their PIRs and IRs, and the rapid identification, prioritization, and action on new IRs. Detailed, well-designed and practiced SOPs understood by all along with continuous coordination and effective C2 of MAGTF intelligence operations will be critical to successfully deal with these challenges.

3007. Evaluate Dissemination Effectiveness

a. General. After disseminating an intelligence product, dissemination leaders should ensure that it was indeed received **and understood** by all intended recipients. Intelligence products occasionally do get misrouted. Also, the individual actually taking the product may not be an intelligence Marine

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

and thus may fail to recognize its importance or, more likely, may fail to inform all needing it or to initiate other necessary intelligence or operations actions. Verification of receipt can be accomplished through a quick telephone call or e-mail confirmation from select addressees. Follow-on contact to determine if intelligence needs were met or if the provided intelligence has led to any new IRs should also be made at some predetermined time following dissemination to ensure optimum use of intelligence. ***Never forget: you must get the operator what he needs when he needs it; in the form he needs it; and ensure it is understood and acted upon – or else the intelligence has little or no value!***

b. During garrison operations, evaluating dissemination effectiveness focuses on:

1. Post-exercise or operations, obtaining detailed after action reports and lessons learned (to include from commanders, operations officers, CIS officers and other key personnel). Analyze all thoroughly, with special attention to critical failures and problems – but also major successes. Identify and implement required improvements (SOPs, training, equipment, personnel).
2. Post-exercise or operations, analyzing of all MAGTF training -- to include questioning of subordinate commanders, other functional area staff planners, and all intelligence personnel - - to assess the validity and currency of dissemination contingency plans and TTP – as well as other related aspects of intelligence operations -- in order to identify root causes of problems and initiate solutions. The departure point for this analysis will be acquiring each supported commander's personal assessment of how well overall intelligence operations, intelligence product formats, and the dissemination system fulfilled his tactical requirements.
3. Preparing and submitting to higher headquarters, the supporting establishment or other relevant organizations comprehensive reports detailing dissemination deficiencies beyond the MAGTF's ability to resolve. Concurrently, if any are particularly significant or complex, active personal involvement by the MAGTF commander may be essential to get necessary corrective actions. Note: Ensure these reports and recommendations are coordinated with and, as required, supported by the G-3 and G-6, to include concurrent actions in their functional areas, as appropriate. Also, ensure these reports are shared with other Marine Corps units, the other services, and the joint community, as appropriate.

c. In response to developing crisis situations, receipt of an alert or warning order, or an actual operational commitment, evaluating dissemination effectiveness focuses on:

1. Executing the plans and actions developed during all prior intelligence operations and dissemination methodology steps.
2. Intelligence collection, production and dissemination leaders maintaining regular communication with supporting and supported commanders and intelligence officers,

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

keeping them apprised as to the status of open IRs, IDRs and ongoing intelligence operations.

3. Continuous, close communications with commanders and planners (to include those of subordinate commands) to ensure disseminated intelligence is understood (especially critical early in operations planning); satisfies their needs; leads to new IRs or changes any previously established priorities; is in forms most supportive of their needs.
4. CMDO and other intelligence personnel periodically seeking assessments from commanders, intelligence officers and staff users throughout the MAGTF regarding dissemination operations, problems, concerns and future anticipated needs.

3008. Train Personnel in Dissemination Tactics, Techniques, and Procedures (TTP) and SOPs.

**Regular and realistic training of all intelligence personnel and users –
commanders, operations, fires, CIS and others -- to improve their understanding of
dissemination operational capabilities and limitations, their tactical abilities and judgments,
and their technical skills and expertise.**

This is the critical unifying action for all dissemination methodology steps -- and one of the most difficult challenges commanders and intelligence leaders will face. Confidence in the MAGTF's dissemination readiness, evaluating its effectiveness, and reaching accurate conclusions as to dissemination strengths and weaknesses will be accomplished only if MAGTF peacetime training aggressively challenges dissemination capabilities under a variety of realistic tactical scenarios and operating conditions. This is particularly critical for accurately assessing whether centralized intelligence management is effectively being supported by the MAGTF CIS system. Training emphasizes units' SOPs, but also other services, joint and intelligence agencies' TTP. The following must be developed, incorporated into the unit SOPs, and practiced in training:

- Ensuring that the intelligence operating concept and supporting dissemination TTP contain detailed procedures well integrated with collections and production procedures, so that during tactical operations dissemination problems experienced anywhere within the MAGTF are immediately brought to the attention of the appropriate personnel for fast corrective action.
- Procedures for maintaining awareness of the current operational status of all key intelligence and multipurpose CIS resources, channels, frequencies, etc.
- Procedures for confirming the receipt of disseminated intelligence.
- For intelligence provided in response to a PIR, using procedures which quickly verify that the PIR has been fully satisfied, and whether it generates any new IRs or affects others

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1 still open.

- 2
- 3 • Ability and expertise of commands, planners and other non-intelligence personnel to
- 4 “pull” intelligence from databases, www sites, publications and other intelligence
- 5 resources.
- 6
- 7 • Tactical and technical abilities of key dissemination and other intelligence leaders (e.g.,
- 8 COC and SARC watch officers) to recognize when, and effectively conduct time-
- 9 sensitive dissemination, to include using non-typical channels, means and modes.
- 10
- 11 • Dissemination to other services, joint, allied/coalition, and NGOs/PVOs.
- 12
- 13 • Integration of intelligence and reconnaissance units’ (e.g., DST, UAV RRS, HET),
- 14 intelligence, C2 and CIS operations into headquarters of all subordinate organizations
- 15 down to the battalion/squadron/CSSD level.
- 16
- 17 • Specialized or unique intelligence dissemination or CIS capabilities – e.g., SCI
- 18 sanitization, CI RODKA, etc.
- 19
- 20
- 21
- 22

Chapter 4

Intelligence Dissemination Planning

4001. Dissemination Planning Process

a. Overview. Intelligence dissemination planning requires broad, multi-functional intelligence, operations, and CIS expertise to successfully identify, analyze, design, coordinate, and integrate a wide variety of complex issues. Dissemination planners must anticipate requirements prior to any exercise, contingency, or operation. The following general principles apply to intelligence dissemination planning:

- Grouping of IRs by type of intelligence and echelon of those needing it is the basis of the intelligence dissemination plan.
- With well-developed intelligence operations SOPs and TTP and established intelligence product formats, training and experience, IDRs can be anticipated and planned for by all intelligence personnel involved with dissemination.
- Finally, effective intelligence dissemination planning emphasizes the importance of integrated collection, production, and dissemination operations requiring continuous close coordination among all intelligence leaders responsible for any aspect of intelligence operations.

b. The Basic Plan. A basic intelligence dissemination plan should be constructed by intelligence officers and their dissemination Marines to use as a MAGTF working model and rapid departure point. From that modifications can be made quickly when developing specific, tailored intelligence dissemination plans to support the spectrum of possible operations. This chapter lays out a process and addresses considerations for use in developing intelligence dissemination plans. Appendix K of this publication provides a sample intelligence dissemination plan format; Appendix G provides a sample intelligence CIS plan format.

c. Considerations. The following paragraphs address the most common considerations for each step of the planning process when developing and implementing intelligence dissemination plans. Although written from the MEF intelligence section perspective, it may be tailored to intelligence officers at any echelon consistent with the policies and TTP of the MEF, other components, JTF, and theater combatant command.¹ Additionally, Appendix H identifies typical dissemination planning and execution actions of the MAGTF CE G/S-2 and Intelligence Battalion staff during each phase of the Marine Corps Planning Process (MCPPE).

¹ Since Marine units may be committed worldwide, it is imperative that MARFOR and MEF dissemination planners periodically coordinate their efforts, concepts of operations and SOPs with each other so that all have a thorough understanding of dissemination SOPs, TTP, policies, capabilities and differences among the various combatant and MARFOR commanders.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

4002. Identify Dissemination Requirements. Validated and prioritized PIRs and IRs drive IDR planning. When identifying requirements, the four W's -- the "who, where, what and when" questions -- provide a good, four-step process for identifying the broad scope of dissemination needs. Direct and continuous communications with dissemination and other intelligence planners at each *who* is essential to precisely focus subsequent dissemination planning efforts. Dissemination requirements depicting type of intelligence and level of recipient can be reflected on a wall mapboard or in a computer file.

a. The Who's. The first step is to identify the *who's*. Commanders' preferences, standing theater OPLAN/CONPLANS, type mission analyses, unit SOPs, TTP, playbooks and previous post-exercise analyses and lessons learned reports all are key sources for identifying the *who's* -- organizations, units and other elements that the intelligence section must be capable of disseminating intelligence to. Identifying and grouping by typical command relationship/task-organization will provide the operational perspective to begin dissemination planning. Determine others who will/may need the support, and not simply those specifically involved with an IR, or immediate higher and lower echelon.

The following portrays a typical MEF dissemination readiness *who* needs:

-- Higher Headquarters, External Intelligence Centers and Other Senior U.S. Government Organizations:

- Joint task force (the J-2 and its key subordinate nodes: JISE, NIST, J-2X, JIDC, JDEC, JCMEC; the J-3's JRC via the MAGTF G-3; the J-6's JCCC via the MAGTF G-6; etc.)
- MARFOR component headquarters G-2 (and other staff sections and nodes, as required)
- Theater combatant command's joint intelligence center (JIC) or joint analysis center (JAC)
- U.S. embassy/country team
- National intelligence agencies (DIA/NMJIC, NSA/NSOC, CIA, NRO, NIMA)
- Marine Corps Intelligence Activity (and other services' intelligence centers, as appropriate)
- Appropriate cryptologic shore support activity (CSSA)
- Appropriate regional security operations center (RSOC)
- Marine Corps Imagery Support Unit (MCISU)
- Allied/coalition partners' military and national intelligence organizations and elements.

- Adjacent or Detached Commands or Organizations:

- Intelligence sections of the Joint Force Land/Maritime/Air/Special Operations Component Commanders (or to those of any of their subordinates)
- Specialized task forces (e.g., Joint Psychological Operations Task Force)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

- Allied, coalition or multinational forces' intelligence sections
- Deployed Marine Expeditionary Brigade (MEB), MEU (SOC), MEF alert contingency force and SPMAGTFs command elements intelligence sections
- Intelligence sections of Army, Navy, Air Force, service component headquarters (and their subordinates, as appropriate)
- Near-real-time (NRT) connectivity to the reporting of intelligence collectors organic to or in direct support of these organizations (e.g., Joint STARS, GUARDRAIL)
- Advance forces
- Appropriate sections/offices of host government, nongovernmental organizations (NGOs) and private voluntary organizations (PVOs)
- Appropriate U.S. law enforcement agencies (during domestic support, counter-narcotics and other designated operations)

- Internal MEF/MAGTF Headquarters

- Current operations center
- Future operations center
- Future plans divisions
- MEF tactical echelons (when deployed)
- Force fires coordination center
- Rear area operations center (when established)
- Civil-military operations center (when established)
- SYSCON
- Rear command echelon

- Subordinate Elements and Units

- Intelligence sections of the GCE, ACE and CSSE headquarters (and their subordinates consistent with the concept of operations)²
- Organic/attached/direct support intelligence, CI and reconnaissance units for whom the MEF retains full command or technical control (TECHCON)³
- Other C2 nodes and facilities, when required (e.g., DASC, EPW compound, POG/AACG/DACG, etc.)
- Other MAGTFs and independent task forces
- Other unassigned subordinate or attached units (e.g., a supporting Army psychological operations detachment)

b. The *Where*'s. The second step is to identify the *where*'s. In most cases this will correspond to the location of each identified *who*. However, command relationships, the specific operational phase, task-organization, or other METT-T factors may identify other answers to *where*

² Dissemination planning to those elements must be closely integrated with specific intelligence alarm and broadcast reporting criteria.

³ Dissemination CIS planning must be well-coordinated and integrated with the CIS established to support intelligence C2 of these intelligence and reconnaissance units.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

dissemination requirements. Intelligence dissemination planners must pay particular attention to special dissemination requirements during any of the following situations:

- Intelligence concepts of operations involving “reachback” or split-base operations.
- Units being globally sourced, not yet OPCON to the MEF or its MSEs.
- Location of unit C2 facilities during tactical operations displacements.
- Whether any unit is or will be collocated with and may benefit from another organization's CIS capabilities.
- Afloat operations and ship-shore movement phases.
- Heliborne or air movement operations.
- Terrain, weather or atmospheric conditions which may affect dissemination.

c. The *What's*. With the above information in hand, dissemination planners now seek answers to the *what* of each requirement, the third step in the process. Here planners strive to establish or anticipate what type intelligence support -- finished deliberate intelligence, time-sensitive intelligence products, particular formats -- each *who* typically requires to support its planning and decisionmaking needs. As with the *who* determinations, commander preferences, standing MAGTF and theater OPLAN/CONPLANS, type mission analyses, unit SOPs, TTP, playbooks, and previous post-exercise analyses and lessons learned reports all are key sources for isolating *what* needs and will provide the dissemination SOP foundation. Then, during operations, these will be modified as required consistent with specific mission needs, the commander's intent (as well as those of higher and adjacent headquarters), concept of operations, endstate, and METT-T. Additionally, planners' research should encompass how differing intelligence resource task-organizations might affect *what* requirements and to how the possible *what's* historically have been combined to satisfy the *who's* requirements. Cross-referencing the *who* and *what* answers with the following groupings completes this step:

- Finished intelligence products (intelligence studies, estimates, reports, etc.)
- Address indicator groups (AIGs), DSSCS address groups (DAGs), collective address designators (CADs), and MAGTF units
- Alarm intelligence support (e.g., I&W reports, time-sensitive target of opportunity reporting, etc.)
- IMINT (to include standard scales, quantities, annotations)
- SIGINT (e.g., requirement for time-sensitive/non-codeword reporting; sanitized version SCI products)
- HUMINT (e.g., CI time-sensitive reports, tactical interrogation reports, special CI reporting)
- GEOINT (e.g., planning and operational map allowance requirements, terrain models and analyses, geospatial information (GI) needed for automated systems)
- Reconnaissance and surveillance (e.g., anticipated requirements as the GCE lead elements advance and deployed ground reconnaissance and ground sensor platoon (GSP) elements' reporting becomes more pertinent to their -- vice MAGTF CE -- current operations)
- Preferred level(s) of classified information that the *who* desires (further subdivided into what they require access to and what they can actually retain on-hand)

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- Releasability and formats for sharing intelligence with allied/coalition partners, NGOs, and PVOs

d. The When's. The final basic dissemination planning step is to determine each *who's* typical or stated *when's* – identifying timeliness requirements. The same sources used to research the previous W's likewise are recommend for acquiring initial *when* answers and baseline planning criteria. The obvious answer is: ***the sooner the better consistent with quality information.*** However, this factor is highly variable during tactical operations. Key planning considerations include:

- Rapidly assessing the feasibility of satisfying the commander's or planner's stated LTIOVs (intelligence already on-hand or accessible? Can organic assets acquire/produce needed intelligence? Will external support be needed?)
- Nature of the IR (i.e., routine dissemination, alarm criteria/time sensitive IDRs, is it a PIR or in support of another CCIR?)
- Communication transmission requirements for the *Who's* desired format (voice, text, digital, bulk delivery, bandwidth, etc.)
- Capabilities and current status of the MAGTF CIS system, to include current CIS status of recipients

4003. Develop the Intelligence and Information Flow

a. Intelligence Flow. Dissemination planning must begin with analyzing the intelligence and information processes, not just drawing boxes for the location of the various automated systems and intelligence nodes. Once the flow of intelligence, in various forms, has been visualized, detailed planning can be worked out. The use of various types of flow diagrams and dissemination planning matrices can assist in the process. Figure 4-1 shows an example of a MEF intelligence support to targeting flow digram. No standard dissemination matrix has been developed for all dissemination planning functions, but some examples are provided in figure 4-2 (Intelligence Dissemination Requirements Planning Matrix) and Appendix J (Intelligence Reports Matrix). When building a MAGTF dissemination matrix, key dissemination recipients, such as the MSCs, must always be depicted.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

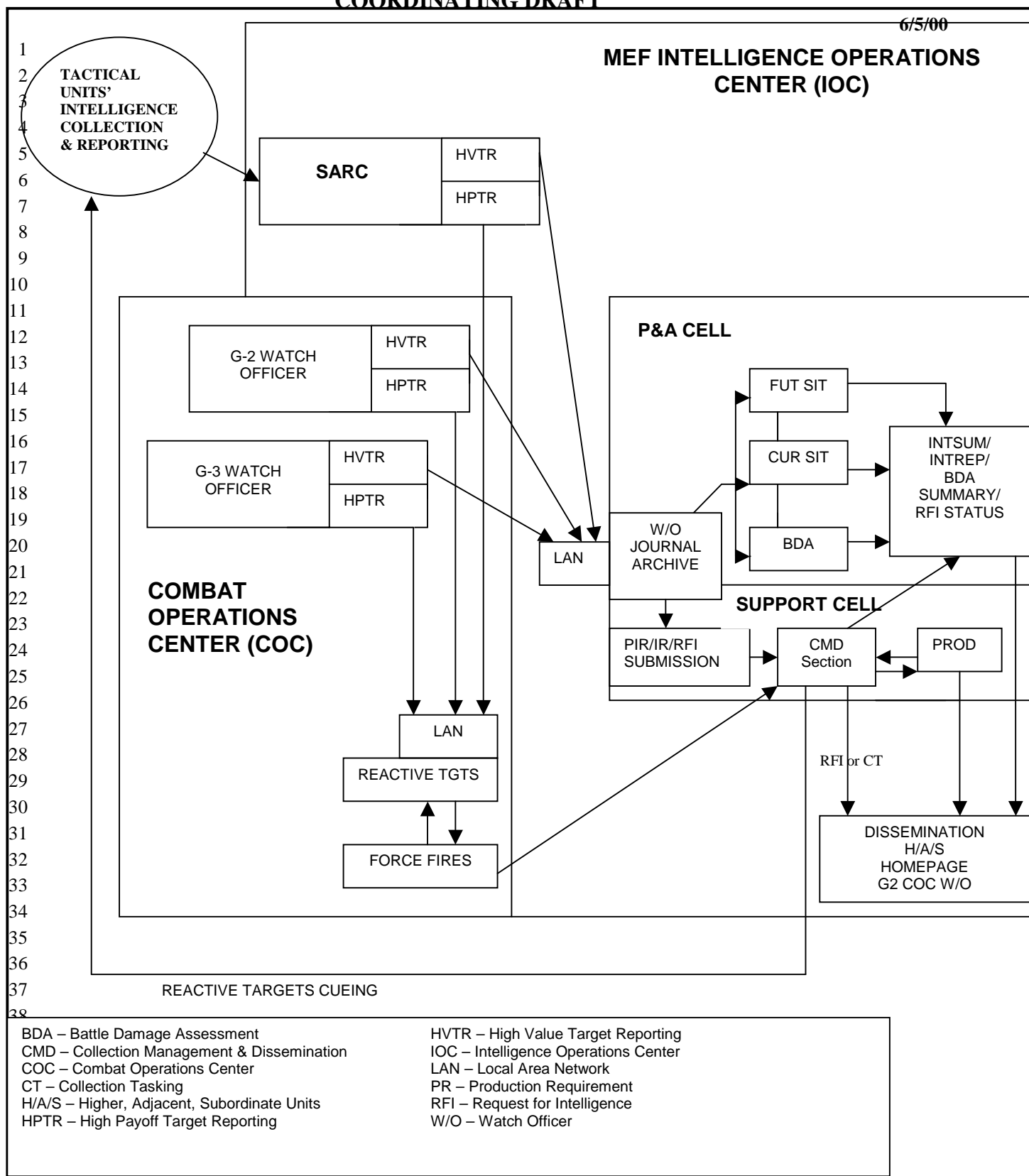


Figure 4-1. Example, MEF Intelligence Support to Targeting Flow Diagram

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Example: Notional MEF Intelligence Support to Targeting Flow

Targeting Related IR Management. Targeting-related IRs will be submitted by higher, adjacent and subordinate elements. These will be submitted to the CMDO in the IOC. The CMDO will consult with P&A Cell and other producers to determine if they can answer the request. If yes, they will do so per either the production or dissemination plan, disseminate products as appropriate, and also post the answer or the product on the intelligence homepage. If the analysts cannot answer the request, they will so notify the CMDO who will then prioritize and request collection.

Support to Time-Sensitive Targeting. Each potential source of time-sensitive targeting intelligence must make decisions on whether the combat information received constitutes high payoff target reporting (HPTR), and if it is targetable. Daily guidance reflecting changes to the commander's intent, G-3 force fires targeting priorities, the daily targeting board and the G-2/IOC's PIRs and intelligence reporting criteria provides this. A tracking and identification code/system should be established for these reports. Reactive targeting occurs when HPTs are located. This time sensitive intelligence is collected and disseminated through the organization responsible for reporting from the sensor concerned. Generally, information will come to the MEF G-2 and its IOC through either the: SARC or the COC intelligence watch (point of contact for friendly unit intelligence and combat information reporting). In special cases and when authorized, this flow may be direct from a specialized intelligence unit to designated recipients (e.g., from RadBn's OCAC to the COC).

Immediate Dissemination of High Value Target Reporting (HVTR). If the information is not an HPT or BDA, it is moved to the P&A Cell for analysis. The P&A Cell will review all reports to determine if it is high value, time sensitive intelligence. If yes, they will note who needs to see it and immediately disseminate it per the dissemination plan and intelligence reporting criteria. If no, it will be determined who needs to see it (internal to the G-2) and used for subsequent intelligence analysis and production.

Analysis and Dissemination of Intelligence Products. P&A Cell analysts will process the information against the current and estimated future enemy situation using other relevant intelligence and databases as appropriate. Time-sensitive intelligence will rapidly be incorporated by the analyst into an Intelligence Report (INTREP) to be disseminated immediately per the dissemination plan and current reporting criteria. Where immediate dissemination is not required, the analyst will likely forward the intelligence for possible inclusion in the Intelligence Summary (INTSUM) or other intelligence products. Where targets are developed through the analytical process, the analysts will forward all targets to P&A Cell's target analysis/BDA team for follow-on support to the targeting process.

b. Intelligence Reporting. An intelligence report matrix depicting standard and time-sensitive reporting guidance should be prepared for every operation. The particular format will be tailored to meet unit/force needs. The matrix should detail the flow of every intelligence report expected to be prepared or handled by the intelligence section and the IOC. For MAGTF elements, this should show the flow from the original reporter (collector, SARC, P&A Cell, etc.) to recipients for each type intelligence report. Appendix J shows an example of an intelligence report matrix.

c. IDR Planning Matrix. The IDR planning matrix is a tool that assists the CMDO in managing the MAGTF intelligence dissemination effort. Using an IDR planning matrix helps keep the focus on the commander's decision points, PIRs and other key IRs. This format may be tailored as needed per unit SOP. Figure 4-2 provides one example, with amplifying information provided below. The following describes the information for each column of the matrix.

Requester: Identify the unit name or staff section who requested the intelligence or products. If the requestor has assigned the IR a control number, also list that here.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

PIR/IR: Identify the supported PIR or IR. This may be either a short text description or its control number.

Likely Collection Timeframe: Can range from “anytime” to specific windows of opportunity for collection (e.g., related to anticipated time phase lines developed during IPR).

Source: Source of intelligence collection. This may be depicted either by intelligence discipline (e.g., SIGINT, ground reconnaissance) or by specific collector (e.g., UAV, EA-6B, HET).

Who Needs Intel First: Most immediate distribution recipient(s). This may be the original requestor, a list of units identified during COA wargaming, etc. – both internal and external to the unit. Note: While good planning will usually identify this, METT-T factors will drive specific instances. Identification may be by unit name, specific node, staff section, or main/supporting efforts.

Timeliness (hours, minutes, seconds): Factor in who need data streams from sensors, who needs full-blown finished analysis, and who needs semi-finished single-source analysis.

Currency (hours, minutes, seconds): Usually there is a direct proportional relationship between timeliness and currency requirements – but not always. Basic intelligence analysts, for example, may need current information for event by event analysis, but their timeliness requirements are less critical than that needed by other analysts and the G-3.

Periodicity of Reporting (days, hours, minutes, seconds, or as event occurs): Usually used when reporting surveillance results or tracking critical threat targets or emerging events. *Nothing Significant to Report* (NSTR) or negative reports are required unless otherwise directed.

General Product Type: Some examples follow:

- Structured text – usually to fill a database or correlator.
- Unstructured text – freeform
- Raw digital stream – usually to fill a database or correlator. (ex. Joint STARS feed the CGS)
- Analog voice
- Digital voice
- Video (tape or digital stream)
- Raster graphic (scanned/bitmapped photos, maps)
- Vector graphic (vector maps, certain “change detection” imagery products)
- Datafiles – usually more than just packages of structured and unstructured text, such as updated programming
- Combination format

Specific/Unique Product Requirements: For each *General Product Type*, identify any specific or unique product or format requirements. Some examples include specific wordprocessing (Word 7.0) or graphics files (.TIF, .JPEG, .BMP) formats, minimum annotations on imagery

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

overlays, etc. This is absolutely critical when designing the MAGTF software applications architecture. You may have to modify procedures when more than one type of application exists across the network or, more typically, when interoperating with coalition/allied partners.

Standard Channels: Identify the primary and first alternate communication channel for routine, non-time-sensitive dissemination (e.g., radio net name, homepage, secure e-mail, secure telephone, courier, etc.).

Alarm Channel(s): Identify the primary and first alternate communication channel for time-sensitive dissemination.

Quantity: Usually only used for hardcopy dissemination. Identify specific quantity for each recipient.

Deliberate Follow-up: Identify if positive personal follow-up is required with any recipient subsequent to dissemination. If so, state who is responsible, with whom and when. Such follow-up is typically required when answering a commander's PIR in order to ensure understanding and to immediately identify any critical new IRs resulting from it.

Acknowledge Receipt Necessary? Yes or No. It's best if the communications data network can do this automatically (like some e-mail packages do).

Keeping a database on subordinate units (based upon historical reliability, preferences and SOPs) which lists much of the above (to include detailed data on alternate paths and channels, IP addresses, e-mail addresses, radio nets, telephone lines, etc.) is essential for dissemination management. Subordinate units must coordinate closely with higher HQ's dissemination planners, providing as much of this data as possible via record correspondence, in order to ensure their needs are most effectively met.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1
2
3

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

4004. Intranet Management

a. General. This section standardizes the management of a MEF intranet. Each staff section is responsible for posting pertinent information to the MEF intranet and ensuring the information is updated and relevant. The MEF Commander's Critical Information Requirements (CCIRs) will frame the type of information that will be posted. This allows information to be shared throughout the MEF and made available to every workstation that has access to a web browser. MSCs will also maintain a web server where both relevant and required information by the MEF can be posted. Invalidated information will not be posted on the web page.

b. Background. An intranet is a communication infrastructure based on the communication standards of the internet and the content standards of the world-wide web. The combination of the MEF web server with those of the MSCs and possibly external agencies that are granted access, forms the MEF intranet. The tools used to create an intranet are identical to those used for internet and web applications. Communications connectivity external to the MEF will be via JWICS, SIPRNET and NIPRNET; internally it is via SCI-TDN, S-TDN and U-TDN.

c. Intranet Management. Relevant information is framed by the MEF CCIRs. The MEF's ability to maintain relevant information on the intranet is determined by its intranet infrastructure and its management roles. The intranet infrastructure relies on five distinct roles for managing the formal content; the web administrator, webmaster, publishers, editors, and authors.

(1) Web Administrator. The web administrator is responsible for facilitating cooperative opportunities among the MEF's various staff sections and administering the MEF's content management infrastructure. The content management infrastructure are those templates and forms that provide the framework for each website. The same person may serve as both the web administrator and webmaster, but it is not recommended. The G/S-6 is responsible for this function.

(2) Webmaster. The webmaster is responsible for the technical infrastructure of the Intranet. The G/S-6 likewise is responsible for this function.

(3) Publisher. Each staff section, based on functional responsibility, will determine what kinds of formal information will be created and maintained by their prospective sub-sections. Although the role of monitoring and implementation may be delegated to another person on the staff, responsibility remains with the section head. Within the MEF CE's G/S-2 and intelligence battalion operations, this function is the responsibility of the ISC.

(4) Editor. The editor determines what official information will be created for specific activities, manages the information creation and updates the process, to include formal review cycles. The P&A Cell OIC performs this function for all intelligence estimates and products posted on the MEF intranet. The Support Cell OIC performs this function for all organic and supporting intelligence, CI and reconnaissance operational products and information.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(5) Author. Authors create the content and actually change and add to the webpages. Each staff section or battlespace function will have authors. Each section head or functional manager will designate authors in writing with a copy to the web administrators. MEF's generally uses two types of pages:

(a) Content Pages. They may be static pages, like the ones you are reading here, or they may be active pages, where the page content is generated "on the fly" from a database or other repository of information. Content pages generally are owned by a staff section.

(b) Broker Pages. Broker pages help users find relevant information. The MEF homepage is a broker page. A hyperlink broker page contains links to other pages, in context. It also may have a short description of the content to which it is pointing, to help the user evaluate the usefulness of the information contained on that page. On the other hand, a search oriented broker page is not restricted to the author's scope, but it also does not provide the same indicators of context to help the user formulate a decision on whether to go to that page.

d. Web Sites. The MEF maintains several websites:

(1) SIPRNET & S-TDN Sites. The MEF maintains a site on the SIPRNET (external to MAGTF) and S-TDN (internal to the MAGTF). This is an intranet approved to handle information classified up to GENSER SECRET. Here you will find information and hyperlinks to homepages for other commands, and ongoing operations.

(2) NIPRNET & U-TDN Sites. The MEF maintains a site on the unclassified intranet located on the NIPRNET (external) and U-TDN (internal). This site can only be accessed by personnel with appropriate authorization. It acts as a conduit for unclassified and official use only information.

e. Formats And Requirements For Operational Web Sites. The formats for operational and exercise websites are standardized to make it easy to locate information and reduce download time. The following guide-lines are germane:

- (1) Web pages will maintain the same look and feel throughout the MEF.
- (2) Text files be converted to html and posted for viewing online whenever practical.
- (3) The web pages and their sub-directories **WILL NOT** be used as "shared drive."
- (4) To reduce download time operational web pages will:
 - Use the minimum amount of graphics necessary to convey the information.
 - Not use background images or frames.
- (5) All pages will indicate the highest classification of information on that page.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(6) MSCs will post the following on their web sites:

- Contact information to include electronic mail addresses and phone numbers.
- Current Operations and Frag Orders.
- Current version of all recurring required reports.

f. Postings of Status Charts to Websites. Status charts (as outlined in Annex U to the OPLAN or OPORD) will be maintained and updated in accordance with the stipulated schedule (at least every four hours at the MEF CE level) on the operational web page by the responsible staff section.

4005. Develop the Dissemination Plan. The answers to the four *W's* can now be translated into the MEF intelligence dissemination plan and supporting plans. In doing this, dissemination planners must maintain close coordination with all intelligence, operations, and CIS officers as well as pertinent intelligence personnel at higher, adjacent, and other external organizations. The goal is to design and implement a plan that is fully integrated with MEF collections and production operations; that will clearly state how the intelligence will be delivered to the requestor; and that allows for sufficient flexibility to adapt to ongoing tactical developments. The dissemination plan must determine both the:

- Physical means of dissemination, and
- Procedures to be followed in transmission.

a. Design and Coordinate the Dissemination Architecture. An intelligence dissemination architecture should be designed schematically so that it depicts links from the source to the recipient. It must depict organizations, type intelligence systems, and CIS connectivity among the forces' (MAGTF, joint, naval) intelligence collectors/producers and the supported decision makers/ planners and C2 nodes. Additionally, it must encompass the different types of intelligence support, from higher headquarters produced all-source intelligence down through the rawer forms of time-sensitive tactical intelligence information. To account for different types of data and intelligence, several linkages may need to be constructed for clarity. Further, since planned dissemination architectures must incorporate sufficient flexibility to adjust quickly to fast-developing tactical circumstances, it must depict both primary and alternate channels for both standard and broadcast dissemination. Chapter 5 of this publication discusses dissemination architecture planning in detail. The following must be incorporated:

- Detail the various means for dissemination: digital networks, radio, wire, and courier communications channels, to include MAGTF common as well as dedicated intelligence systems and architectures. Close coordination with unit G/S-3 and G/S-6 personnel is critical.
- Provide primary and alternate plans for pipeline (routine), alarm (time-sensitive), supply-push (critical), and demand-pull capabilities.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

- Account for different types of data/intelligence, to include that requiring special or unique security controls (e.g., SCI, RODKA, etc.).

The ISC has principle staff responsibility for dissemination architecture. The line of departure for planning is to clearly state IDR architecture needs. In order that the sum of these are seen in context, architecture needs should be stated within the broader intelligence C2 and CIS requirements, approved by the G-2 and the commander, and then provided in a prioritized list to appropriate G-3, G-5 and G-6 planners. Tailored copies should also be provided to higher and subordinate intelligence officers to support collaborative detailed planning.

b. Establish Dissemination Procedures. Comprehensive MEF-wide integrated intelligence/operations/fires/CIS policies and procedures are mandatory if intelligence dissemination is to be effective. General dissemination procedures should be established for the delivery of intelligence from the controlling producers or agencies. The precedence of transmission-- ranging from routine to flash--should be agreed upon by all involved parties in advance. Audiences should be predetermined as well by defining broadcast parameters (i.e., general or specific). Further, irrelevant intelligence can be better eliminated if reporting thresholds and filters are identified early.

At a minimum, dissemination TTP must:

- Clearly identify dissemination responsibilities of the various intelligence staff officers, cells, and centers.
- Coordinate formats for the various types of intelligence products.
- Integrate and coordinate procedures between the intelligence section and other staff sections.
- Develop detailed intelligence reporting criteria, filters and reporting methodologies.
- Detail procedures for both routine and time-sensitive dissemination.
- Identify procedures and means for recording dissemination and related information to aid with management and rapid problem-solving.
- Describe procedures and means for maintaining awareness of the operational status of all MAGTF common and dedicated intelligence CIS.

c. Keep Practical Guidelines in Mind. Common sense and lessons learned, such as the those offered below, should factor into dissemination planning decisions.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(1) General

- Safeguarding intelligence knowledge, successes and challenges from the enemy is an essential consideration.
- Dissemination operations must focus on the importance and quality of the intelligence rather than its volume. Measures that help reduce the volume of intelligence traffic include limiting routine reporting, setting filters to rapidly identify and eliminate information not pertinent to the tactical situation, and establishing minimal reporting thresholds for the generation of intelligence reports.
- Dissemination plans must permit two-way communication, providing means for subordinate units to pass along data, information and intelligence that they collect or develop which identifies new enemy vulnerabilities or enhances situation development for the entire force.
- Intelligence dissemination will be via secure communication means. However, the overriding consideration is always the needs of the supported commanders. Finding the proper balance between security and wider dissemination is a matter of seasoned judgment based upon the tactical situation, the nature of the intelligence, and the sources involved.
- Besides the tactical situation, the form intelligence takes – report, graphic, etc. – has the greatest influence on how and to whom it is disseminated.
- Regardless of how intelligence is disseminated, each occurrence must clearly identify the time of intelligence (TOI) so that recipients can place it in context and rapidly assess its pertinence despite inevitable delays in receipt and during high tempo, high information volume situations.
- Who is authorized to approve the dissemination of any intelligence product or report is a critical determination that must be clearly identified and closely supervised in order to control traffic volume while also minimizing confusion (e.g., circular reporting).
- Most dissemination will occur via common, multi-functional communication means. Support for intelligence purposes via dedicated means must be identified clearly and early, and well-coordinated with all affected organizations.
- Single-source intelligence reporting will usually be from the collector to the appropriate intelligence C2 node (e.g., the SARC, the ROC, the OCAC or the COC intelligence watch) unless otherwise directed in the specified reporting criteria.
- Automated software application standards must be established throughout the force. Dissemination planners must positively confirm, prior to operations, that all supported units and sections have these in order to preclude interoperability problems.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

(2) Push/Pull

- Critical intelligence (chemical-biological weapons employment, surface-to-surface missile attack, etc.) must be rapidly pushed and receipt confirmed with all recipients.
- Pull is used for dissemination of standard intelligence products, such as INTSUMs, generally to meet IRs of many users or to support more deliberate planning needs.
- If users do not have SIPRNET/JWICS or reasonable capacity TDN capability, then they must be considered as lacking a push/pull capability.
- Even if we have good digital network capability, it must be remembered these systems experience problems and can be degraded or disrupted for many reasons. Back-up or alternate means to disseminate must be planned for to replace pull capabilities when necessary.
- Intelligence databases, homepages – dissemination planners must identify what is posted on homepages, down to what level, how often updated, who manages and how in order to effectively manage dissemination, minimize confusion, and ensure sufficient CIS support for all concerned.

(3) E-mail

- When using e-mail for official dissemination, it should be from/to official unit by section or billet accounts (such as Watch Officer to Watch Officer). Individual/personal e-mail accounts should be used only for routine coordination and communication.
- When using e-mail, do not assume transmission equals receipt by all users. Tactical displacements, network problems, etc. all can disrupt timely receipt. Likewise, automated delivery confirmations do not mean that e-mails have been received by intelligence recipients. Accordingly, when using e-mail for intelligence dissemination, originators must assess the criticality of the intelligence versus METT-T and when critical, implement positive confirmation procedures (e.g., secure telephone) to verify its receipt and understanding.
- Setting up accurate address books for e-mail distribution is critical in successful dissemination. Billet titles/personnel names and associated internet protocol (IP) addresses must be 100% accurate for all to whom dissemination may be required.
- Avoid repeated, multiple dissemination of the same reports and information. Also, tailor dissemination vice routinely broadcasting it to a large group of addressees. This degrades CIS and the whole dissemination system. Example: The SARC, P&A Cell, and COC intelligence watch officers all send the same lengthy intelligence report to the same group addressees just to be sure it got to them.
- A list of e-mail account passwords should be maintained and controlled by dissemination managers.
- Standards should be established for the size of files that may be attached to e-mails. When these must be exceeded, approval authority should be restricted in order to maintain discipline. Also, files attached to e-mails must always be scanned for viruses prior to dissemination.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

(4) Intelligence Homepage Dissemination

- You can't put everything on the homepage because it becomes too unmanageable and not everyone has access to SIPRNET or TDN.
- You must determine how to manage it and apply a policy of frequent inspection. Someone must be designated to view each branch's section to scrub for relevancy, easy accessibility.
- You need to work out the layouts of the homepages with the MAGTF G/S-6 or Information Management Officer. Intelligence dissemination via homepage may be best organized by subject; but the Information Management SOP or appendix may direct organization by chronological receipt. Working out these issues ahead of time makes all the difference.
- Decide whether to have a newsgroup or not.
- Standards and guidelines must be articulated on how to monitor homepage dissemination for confirmation of dissemination (e.g., Will you use liaison officers?).

(5) COMSEC Aspects. The effectiveness of disseminated intelligence depends on the ability to maintain security and conceal intelligence techniques and success from the adversary. Accordingly, the commander must provide adequate protection to prevent the capture of intelligence facilities and personnel. In addition, intelligence couriers must be adequately protected, and positive measures must be taken to conceal courier runs and routes. Other COMSEC planning considerations include:

- Coordinate with the appointed special security officers (SSOs) in all units authorized to receive and use SCI.
- Adhere to SCI security handling, processing, and storage requirements.
- Obtain authority and establish procedures for the sanitization of SCI products, reports and other information.
- Determine and coordinate SCI and GENSER LANs and WANs and unique intelligence requirements.
- Determine and coordinate both SCI and GENSER courier requirements and operations.
- Determine unique COMSEC material system (CMS) requirements for intelligence and SCI communications.
- Determine communication requirements between TSCIFs, mobile SCIFs, supporting security forces, and supported units.

4006. Allocate Resources. The intelligence officer--in concert with the unit's communications officer--should allocate available personnel and equipment resources to support dissemination requested. For critical deficiencies, global sourcing should be pursued. Requirements must be estimated and resources allocated for routine and time-sensitive operations, with sufficient redundant capabilities for each. For additional discussion, see paragraph 3005.

The allocation of intelligence resources is most critical during mission execution. A detailed and well-thought-out concept of intelligence support (to include dissemination support), developed in accordance with the commander's intent and concept of operations, will provide an appropriate allocation of dissemination capabilities between the main effort and supporting efforts and

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

between the intelligence support to execution of current operations and the continuous planning effort for future operations. It is particularly important that Marine Corps force (MARFOR), MAGTF, and major subordinate commanders who control the tasking of intelligence units and capabilities provide access to critical intelligence resources for their subordinate elements.

4007. Monitor Execution. Intelligence dissemination will be occurring continuously; it is critical to constantly evaluate its effectiveness, the quality of support to all subordinate commanders, and the rapid identification and resolution of problems.

- Develop a dissemination tracking matrix to record receipt of major/critical intelligence and products by intended recipients. (See figure 4-3 for an example of a dissemination tracking matrix.)

UNIT	WatchO		HQ BN		G-1		TAC		MOBILE		G-3		G-4		G-6		2d MAR		6 th MAR	
PRODUCT	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	rec	sent	re

Figure 4-3. Sample, Dissemination Tracking Matrix

- Determine if the user is satisfied with the quality and quantity of intelligence.
- Supervise adherence to specified dissemination priorities and reporting criteria.
- In particular, ensure that no precedence abuse exists or information overload occurs to degrade or overload communication channels.
- Maintain awareness of the operational status of all supporting CIS, as well as the status of PIRs, IRs and IDRs, in order to rapidly make necessary changes consistent with ongoing operations and METT-T.

Chapter 5

MAGTF Intelligence Dissemination Architectures

“The success of any crisis deployment hinges on the existence of a reliable command and control system and of a flexible, reliable system for gathering, analyzing and disseminating strategic and tactical intelligence.”

-- General H. Norman Schwarzkopf, USA¹

5001. Introduction. CIS architectures provide a framework of C2 functional and technical relationships for achieving access, interoperability and compatibility among military and supporting C2 personnel, nodes and systems. Each MAGTF operational architecture is the basis from which the *systems and technical* aspects of intelligence dissemination is visualized and planned. However, MAGTF intelligence dissemination plans must be continually tailored, updated, and adapted to reflect specific METT-T factors, and must include those aspects of intelligence dissemination which are not CIS-based (such as couriers).

This chapter provides doctrine and TTP principles, methodologies and notional architectures to assist in MAGTF intelligence dissemination CIS architecture planning. It discusses principal C2 nodes, lists CIS objectives and planning goals, explains intelligence CIS architecture planning methodology, and provides brief descriptions of basic intelligence CIS requirements. Appendix I provides notional MAGTF intelligence CIS architectures for integrated all-source intelligence operations.

5002. Background. Intelligence architectures are one part of the broader MAGTF C2 support system. They provide the means to interconnect national, theater, JTF, multinational and other intelligence and reconnaissance operations with the MAGTF's internal intelligence architecture and operations in order to plan and direct, collect, produce, disseminate and use intelligence in support of MAGTF needs. Such architectures are based upon joint and Service doctrine defining operational, organizational and functional missions, command relationships, C2 concepts of operations, and information needs and exchange requirements.

The MAGTF intelligence effort is heavily dependent upon secure, reliable, fast and far-reaching CIS support to receive JTF, other components, theater, and national all-source intelligence, and to transmit organically collected and produced intelligence products and reports throughout the MAGTF. CIS are also required for the command and control of MAGTF and supporting intelligence units and their integration with other intelligence and reconnaissance operations. Every MAGTF mission and situation -- METT-T -- is unique, requiring some modifications to the supporting CIS architecture. Generally, the focus of effort prior to the execution phase of an operation is on JTF/theater/national assets in support of planning. Upon execution, the focus

¹ General H. Norman Schwarzkopf, USA, USCINCENT, Operation Desert Storm, 1991.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

shifts to tactical intelligence, reconnaissance and surveillance efforts and support to subordinate elements. Detailed planning and close coordination between the MAGTF G/S-2, G/S-3, and G/S-6, and all pertinent operational and intelligence organizations is critical for establishing reliable and effective intelligence CIS support.²

5003. Intelligence and Related C2 Nodes

a. References. The intelligence CIS architecture for any given operation is dynamic and heavily METT-T influenced. Key references with respect to specific theater or MAGTF operations include:

(1) Combatant command, JTF and MAGTF intelligence plans developed for various OPLANS.

(2) MAGTF command element intelligence standing operating procedures and combatant commanders intelligence TTP.

(3) Annexes B (Intelligence), C (Operations), J (Command Relationships), K (Communications and Information Systems), and U (Information Management) of the MAGTF and JTF OPLANS and OPORDs.

b. MAGTF Intelligence CIS and External Organizations.

(1) National Intelligence Support Team (NIST)

(a) All-source national intelligence agencies' assets may deploy in support of JTF (and even directly in support of MAGTF) operations as well as providing critical support via reachback and collaborative capabilities. The NIST is the most typical method used. The NIST is a task-organized unit generally consisting of Defense Intelligence Agency (DIA), National Security Agency (NSA), Central Intelligence Agency (CIA), and, as appropriate, National Imagery and Mapping Agency (NIMA) personnel and equipment. Its mission is to provide a tailored, national level all-source intelligence team to deployed commanders (generally at the JTF headquarters level, but support could be provided to other commands) during crisis or contingency operations. Depending upon the supported unit's requirements, a NIST can be task-organized to provide coordination with national intelligence agencies, analytical expertise, I&W, special assessments, targeting support, streamlined and rapid access to national intelligence databases and other products, and assistance facilitating RFI management (see figure 5-1).

² See MC WP 6-22, *Communications and Information Systems*, for a detailed review of MAGTF communications and information systems (CIS) and supporting tactics, techniques and procedures.

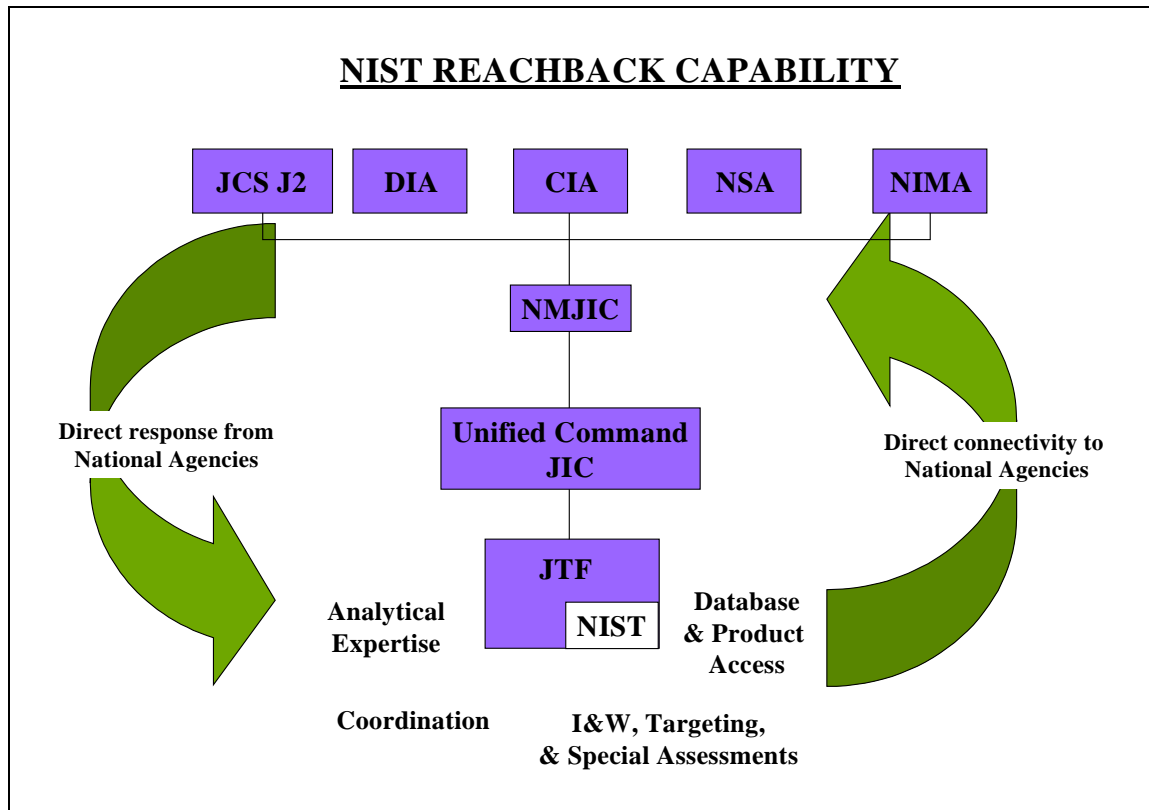


Figure 5-1. National Intelligence Support Team Capabilities

(b) DIA, through the joint staff J-2, controls the NIST for deployment and administrative purposes (see figure 5-2 for an overview of a NIST's deployment cycle). During operations a NIST will usually be in direct support of the joint force commander (JFC), who exercises C2 of it via the JTF J-2. Once deployed, any of the intelligence agencies with representatives on the NIST can provide its leadership. The basic C2 relationship between the NIST and the JTF (or other supported commands) is direct support. The NIST will be under the staff cognizance of the JTF J-2, performing intelligence support functions as so designated. The basic NIST concept of operations is to take the J-2's RFIs and collection and production requirements, discuss and deconflict these internally within the NIST to determine which element(s) should take these for action. Each NIST element leader, and as coordinated by the NIST team chief, will conduct liaison with their parent national intelligence organization. All intelligence generated by the NIST is available to the JTF J-2 joint intelligence support element (JISE), the JFC, and other elements of the JTF with the usual restriction based on clearance and programs.

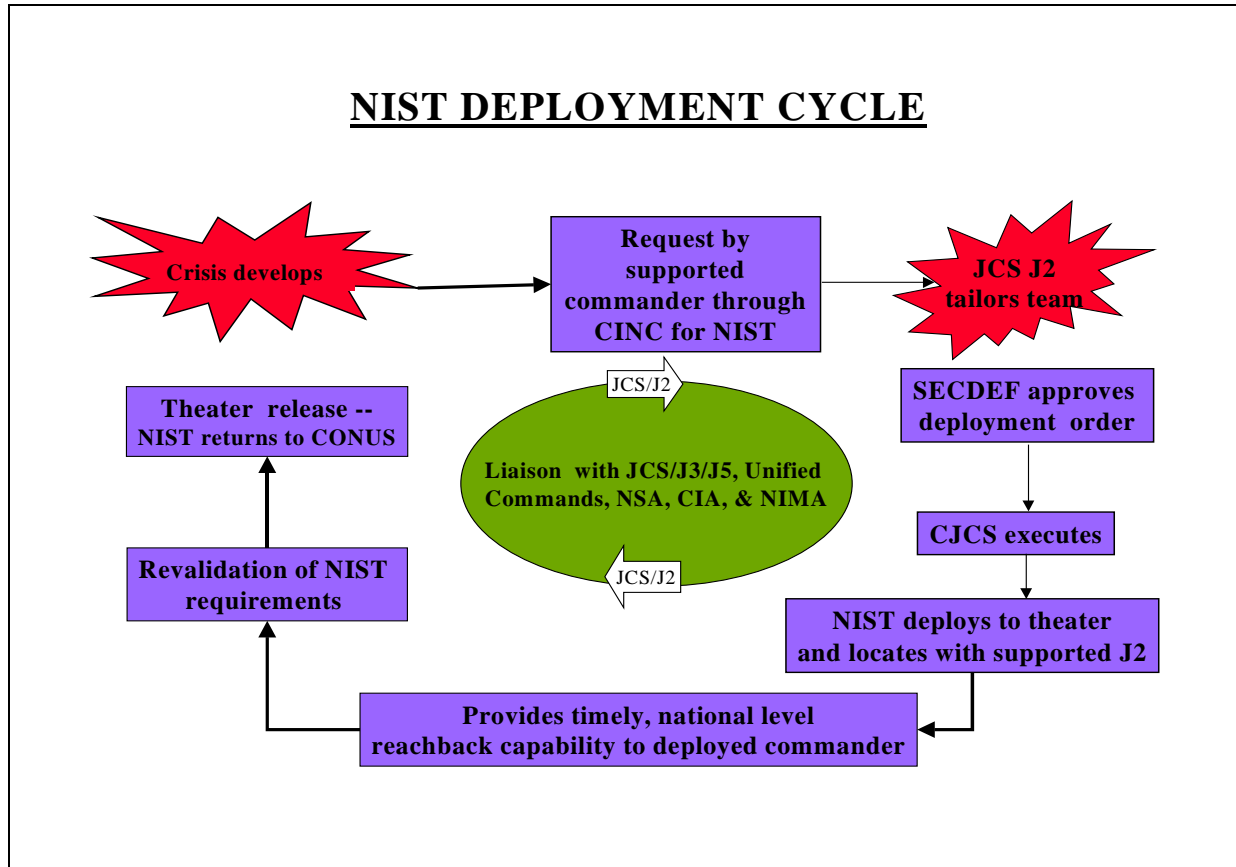


Figure 5-2. NIST Deployment Cycle

(c) The composition and capabilities of each NIST deployment is unique based on the mission, duration, agencies' representation, and capabilities required (see figure 5-3). A NIST, however, is not a totally self-contained element. Rather, it requires logistic and other support from the supported command. Depending upon the situation, support that a NIST may require from the supported unit includes information systems technical support and an access controlled secure area (generally within the supported unit's tactical sensitive compartmented information facility, or TSCIF).

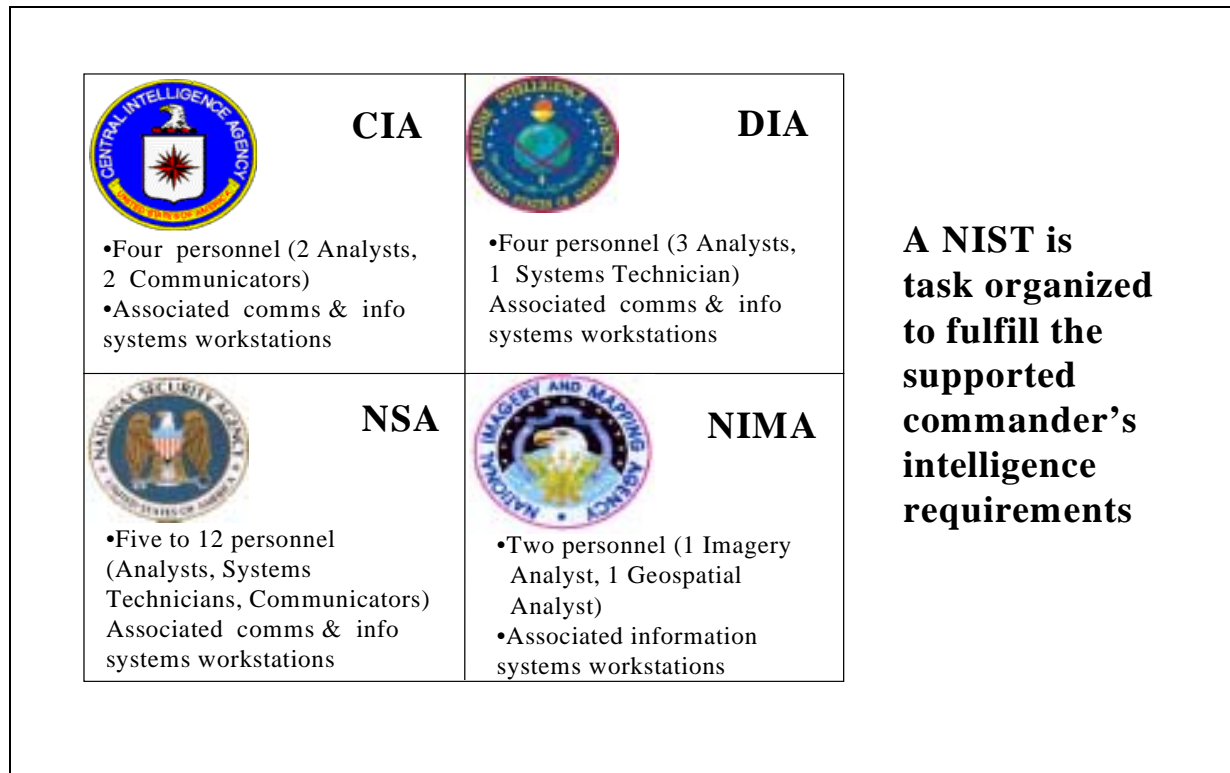


Figure 5-3. Notional Composition of a National Intelligence Support Team

(d) A NIST's organic capabilities generally encompass only intelligence and some unique CIS support. NIST CIS capabilities will be task-organized. It may range from a single agency element's voice connectivity to a fully equipped NIST with JDISS and JWICS video teleconferencing (VTC) capabilities (see figure 5-4 for one of a NIST's key sophisticated CIS capabilities). Current methods of operation continue to rely on both agency and supported command-provided communications paths to support deployed NIST elements. The systems that each element is capable of deploying are discussed in greater detail in appendix C, "NIST Systems", of Joint Publications 2-02, *National Intelligence Support to Joint Operations*.



Figure 5-4. NIST JWICS Mobile Integrated Communications System

(2) JTF J-2 and the Joint Intelligence Support Element (JISE)

(a) The JTF J-2 organizational structure and capabilities will be situation and mission dependent as determined by the JFC and the JTF J-2. The JISE is the principal intelligence C2 node within the JTF J-2. The JISE is the focus for JTF intelligence operations, providing the JFC and component commanders with situational awareness and other intelligence support regarding adversary air, space, ground and maritime capabilities and activities. Figure 5-5 depicts a generic joint intelligence architecture.

(b) All intelligence collection, production and dissemination activities will be conducted within the JISE. Once initial basic and current intelligence products and support have been provided to the JTF and its components, updates will be accomplished by the JISE using push/pull dissemination techniques. Intelligence CIS based on the JDISS/JWICS functionality provide the JTF with the ability to query theater and national intelligence servers and databases for the most current intelligence. (See Joint Publication 2-01, *Joint Intelligence Support to Military Operations*, and Joint Pub 2-02, *National Intelligence Support to Joint Operations*, for additional information on national and JTF intelligence operations.)

(1) Collection. The JTF J-2 collection manager will plan, coordinate and direct intelligence operations in support of the JTF and subordinate components. A wide range of theater and JTF collection assets may be employed. Depending upon the situation, specific

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

collection missions, and time-sensitivity of the collected information, MAGTF interfaces with these external collection operations may be direct between the MAGTF CE and the collector (e.g., between Joint STARS aircraft and intel bn's Joint STARS common ground station) or will support will be received post-mission via the established JTF CIS architecture.

(2) Production. MAGTF IRs will be managed by the JISE in accordance with the JFC's PIRs and other validated IRs. Connectivity is provided via the established JTF CIS architecture -- principally JWICS and SIPRNET -- and MAGTF production elements.

(3) Dissemination. Once basic and current intelligence have been provided to a deploying JTF and its components, updates and new intelligence will be accomplished using push/pull dissemination techniques. Intelligence CIS based on the the JTF JDISS/JWICS/SIPRNET and the MAGTF's IAS/SCI-TDN/S-TDN architecture provide the JTF with effective interoperability and the ability to query theater and national intelligence organizations, servers and databases for the most current intelligence.

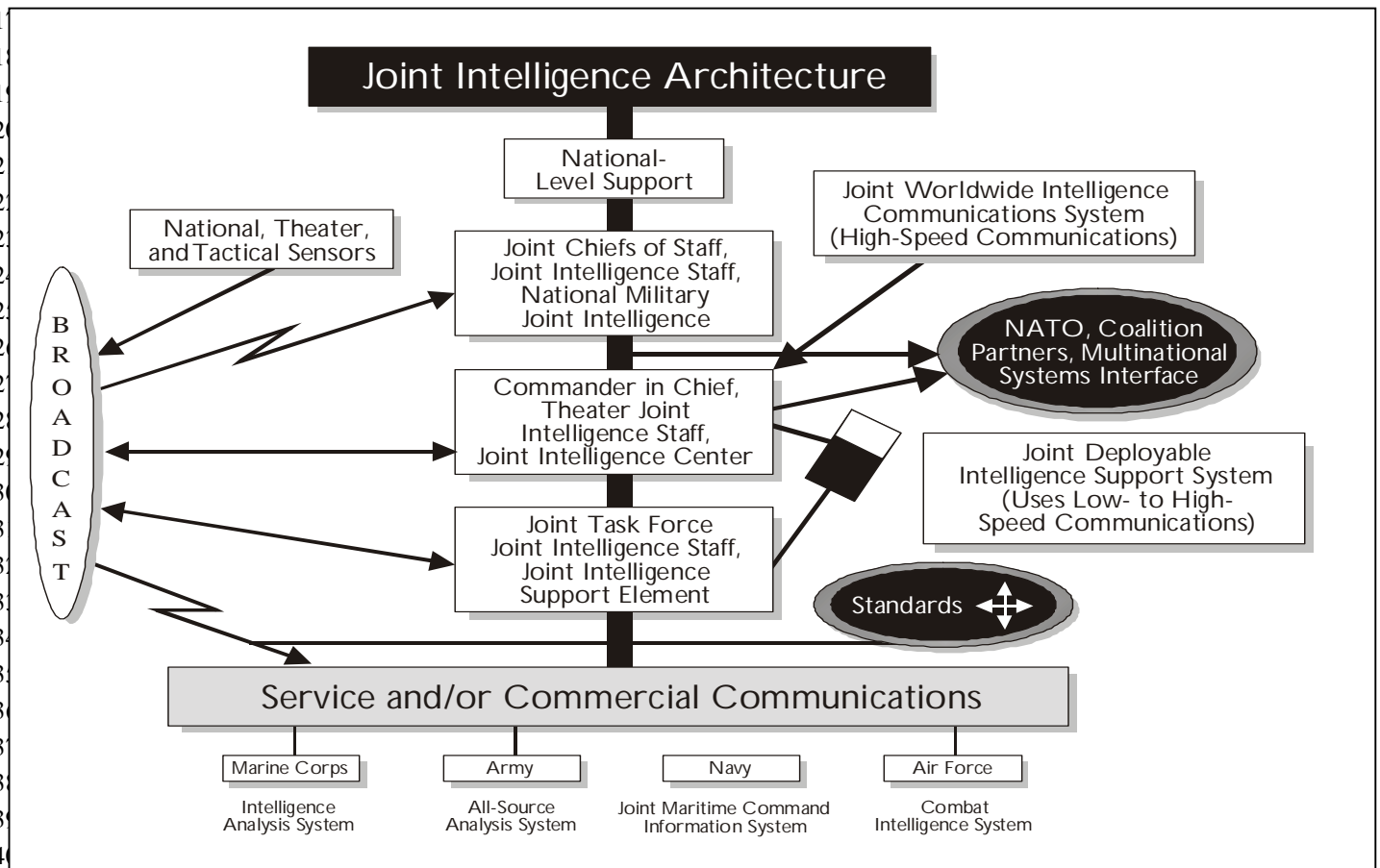


Figure 5-5. Joint Intelligence Architecture

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(3) Theater, Combatant Commands' Joint Intelligence/Analysis Centers (JIC/JAC).

The combatant commands' JICs and JAC are the cornerstones for fulfilling the IRs of the geographic combatant commanders and their subordinate commanders. The JICs and JAC are the primary source from which subordinate JTFs receive intelligence support for their areas of interest, providing finished intelligence products in support of theater mission planning and execution.

w Collection. The combatant commander's J-2 retains full collection management authority (i.e., to validate, modify, or non-concur) over all intelligence collection requirements against targets within their area of responsibility. Such authority may be delegated to a subordinate JFC. All validated collection requirements that cannot be satisfied by organic JTF means will be submitted to the combatant command's JIC/JAC.

w Production. Combatant commands, services and defense agencies intelligence production centers' production responsibilities are clearly delineated within the DOD Intelligence Production Program (DODIPP). The DODIPP is structured to capitalize on the analytical and production resources of the entire DOD intelligence production community. It supports the efficient use of production resources, prevents duplication of effort, and enhances timely support to user IRs. The Community On-Line Intelligence System for End-Users and Managers (COLISEUM) automates DODIPP procedures for stating and tracking theater IRs and other intelligence production requirements. Results may be incorporated into all-source or single-source intelligence products, or into various intelligence databases. MAGTF access to these will be via the procedures described earlier and the established JTF CIS architecture.

w Dissemination. The Joint Deployable Intelligence Support System (JDISS), using principally JWICS for connectivity, is the primary intelligence system used by the JIC/JACs for both the receipt and dissemination of intelligence products. Using these systems, multimedia intelligence dissemination (voice, data, imagery, record message, e-mail, graphics, video) can be supported. File servers maintained by the JIC/JACs are key components of intelligence support. These file servers can be accessed using JDISS and IAS, providing subordinate commands and other users the ability to pull intelligence when required. The JICs have access to all of the government-owned, common user networks used by the intelligence community: Defense Message System (DMS), Defense Special Security Communications System (DSSCS), NIPRNET, SIPRNET, JWICS, and the Defense Switched Network (DSN). Access to military satellite systems includes the Defense Satellite Communications Systems (DSCS) and the Fleet Satellite Communications System (FLTSATCOM). Commercial satellite access is also available through the International Maritime Satellite System (INMARSAT) and INTELSAT.

(4) Multinational Operations. Combined and multinational operations are today the norms, making critical the sharing of intelligence between the MAGTF and allies. There is no existing multilevel security system to facilitate the automated dissemination to combined or multinational partners of disclosable and releasable intelligence or geospatial information. Combatant

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

commands and subordinate JTFs can request through DIA, NIMA, NSA, or CIA that intelligence information be either disclosed or released to coalition and/or allied nations as necessary. A subordinate joint force must be interoperable with, and have access to, theater intelligence databases, as well as allied and/or coalition force databases and dissemination systems. For example, intelligence products may be stored on systems such as the Linked Operational Intelligence Centers Europe (LOCE), the primary automated system for exchanging information with North Atlantic Treaty Organization allies. A similar capability exists in Korea with the Pacific automated data processing (ADP) Server Site - Korea.

(a) **Planning.** When planning CIS requirements, the combatant command/JTF J-2 identifies the type of mission, formulates the concept of operations, considers joint and service doctrine, and determines the specific mission requirements. The MAGTF G/S-2 must work closely with the J-2 and J-6 and, in the case of a JTF, with subordinate commanders, to determine intelligence CIS data bandwidth requirements, recommended priorities of data transmission, and the development of primary and alternate plans. Supporting communications paths will require connectivity with the Defense Information Systems Network (DISN) to allow for the transmission of large (especially GI /GEOINT/imagery) files.

(b) **Mission Objectives.** As specific mission objectives of the JFC and each of the subordinate component commanders are developed, the JTF J-2 develops a list of the subordinate joint force intelligence assets and those assigned from national and service sourcing. The MAGTF G/S-2, with the specific activity timelines for planned operations, will produce an estimate of the data bandwidth and other CIS requirements necessary to fill shortfalls in intelligence data transmissions.

(c) **CIS Plan.** The JTF J-6 determines the specific CIS plan to support intelligence operations throughout the to the MAGTF and to adjacent/higher commanders. The plan will include a node-to-node layout of existing and planned data transmission routes and the identification of all organizations or units to be included in the communications architecture.

(5) Amphibious Task Force Intel Center (AFTIC). During amphibious operations, amphibious task force (ATF) and the MAGTF's CE intelligence sections generally will integrate their operations. The principal intelligence C2 node is the AFTIC located aboard the ATF flagship. The ATFIC is composed of designated shipboard spaces with installed CIS systems that support the intelligence operations of both the ATF and landing force (LF) while reducing duplicative functions and producing more comprehensive and timely intelligence for the entire naval task force. Standard CIS connectivity is available – JWICS, SIPRNET, NIPRNET, AUTODIN, DSN. Access is provided via the flagship's GENSER communication center and the special intelligence communication center within the ATFIC's ship's signals exploitation space (SSES). Embarked intelligence specialists with associated equipment must be integrated into the CIS network for access to the ship's communication capabilities for receipt and dissemination of intelligence. Coordination with the ship's communication officer is critical to support access to the national production network and distributive production support. Access is necessary for pulling intelligence and data from support facilities and for "pushing" tailored mission products

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1 to embarked LF elements and forward to support LF operations ashore using split-based,
2 reachback and other methodologies.

3
4 **c. Principal Intelligence C2 Nodes.** The following are the principal C2 nodes from which
5 MAGTF intelligence operations are planned and directed:

6
7 **(1) MEF Command Element Intelligence C2 Nodes -- Combat Intelligence Center and**
8 **Intelligence Operations Center.** The CIC and its subordinate elements is the principal MAGTF
9 intelligence C2 node that provides the facilities and infrastructure for the centralized planning,
10 direction and C2 of the MEF's comprehensive intelligence, CI and reconnaissance operations
11 (see figure 5-6). Since the CIC must effectively support the *entire* MAGTF, it must remain
12 responsive to the requirements of *all elements of the MAGTF*. Understanding the CIC and its
13 subordinate elements is essential to effective intelligence C2 and planning, integrating and
14 executing effective intelligence collection, production and dissemination operations.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

Combat Intelligence Center (CIC)—overarching intelligence operations center established within the MEF or MEB main command post. Encompasses the primary functions of the MEF intelligence section and Intelligence Battalion. It includes the following sub-elements.

G-2 Plans—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE future plans team; and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.

G-2 Operations—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE CG, battle staff, current and future operations center elements; target intelligence support to force fires operations; G-2 section intelligence requirements management activities; Red Cell support; and MEF intelligence liaison with external commands and organizations.

Intelligence Operations Center (IOC)—principal MEF intelligence operations and C2 center that is established by Intel Bn. Performs intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence analysis and production, and intelligence dissemination. It includes three integrated, mutually supporting intelligence operations cells:

- * **Support Cell**—primary element for conducting MEF-wide intelligence requirements management; weather support; collections and dissemination planning and direction; and intelligence staff cognizance of MEF organic and supporting intel and recon operations.

- * **Production and Analysis (P&A) Cell**—primary analysis and production element of the MEF. Processes and produces all-source intelligence products in response to requirements of the MEF. Additionally, it is the principal IMINT and GEOINT production element of the MEF.

- * **Surveillance and Reconnaissance Cell (SARC)**—primary element for the supervision of MEF collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.

CI/HUMINT Company Command Post—primary element for conducting CI/HUMINT planning and direction, command and control, and coordination of MEF CI/HUMINT operations with external CI/HUMINT organizations.

Operations Control and Analysis Center (OCAC)—main node for the C2 of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations. Processes, analyzes, produces, and disseminates SIGINT-derived information and directs the ground-based electronic warfare activities of the radio battalion.

Reconnaissance Operations Center (ROC)—main node for the C2 of force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations. Processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

Figure 5-6. MEF CE's Combat Intelligence Center and Intelligence Battalion's Intelligence Operations Center Key Elements

1
2
3

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

In supporting this objective, the CIC supports both G-2 section and intelligence battalion operations. While integrated, the organizational approach differs some for each of these.

w G-2 Section. The G/S-2 serves as the intelligence officer for the MAGTF commander, with the CIC serving as the primary intelligence C2 and operations node for the *entire* MAGTF. As such, the CIC *must* remain responsive to the requirements of *all elements* of the MAGTF. In this intelligence support concept, the CIC provides the facilities to allow the MAGTF intelligence section and intel bn to perform the following tasks:

- (a) Provides centralized direction for MAGTF intelligence operations.
- (b) Consistent with the commander's priorities, consolidates, validates, and prioritizes IRs of the entire force.
- (c) Plans, develops, and directs the MAGTF collection, production, and dissemination plans and operations.
- (d) Maintains a consolidated, all-source production center in the MAGTF P&A cell.
- (e) Directs the employment of MAGTF organic collection assets through the SARC and the operations control and analysis center (OCAC).
- (f) Submits consolidated requests for external intelligence support through the Marine component headquarters to appropriate agencies.
- (g) Links the MAGTF to national, theater, joint, other-Service, and multinational intelligence assets and operations.

The key G-2 section nodes are organized to effectively align and support the MEF CE's staff cross-functional cellular staff organization and concept of operations. The G-2 plans branch is aligned to provide intelligence support to the MEF CE's future plans cell efforts. The G-2 operations branch is aligned to provide intelligence support to the MEF CE's COC, FOC, force fires center and to direct and manage the G-2's Red Cell and the MEF's external intelligence liaison teams (see figure 5-7).

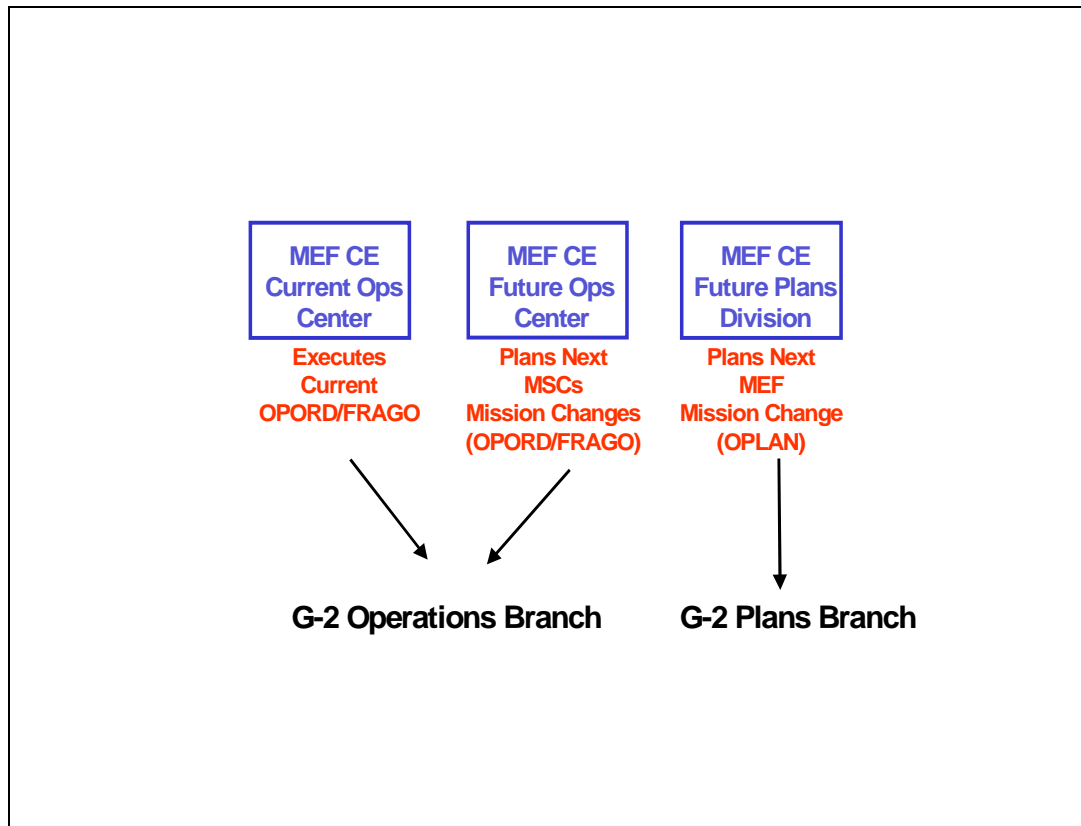


Figure 5-7. MEF CE Cross-Functional Cellular Organization and Intelligence Support

CIS facilities, CIS and other support must allow the AC/S G-2 and G-2 section to perform the following major tasks:

- (a) Developing and answering outstanding MEF and subordinate units' PIRs and IRs by planning, directing, integrating and supervising MEF organic and supporting intelligence, CI and reconnaissance operations.
- (b) Planning the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and concept of operations.
- (c) Recommend CI and force protection measures and countermeasures.
- (d) Preparing appropriate intelligence plans and orders for the MEF, to include reviewing, coordinating, and integrating the intelligence plans of JTFs, theaters, and other organizations.
- (e) Coordinating, providing and facilitating the use of intelligence to the MEF CG, the battlestaff, the future plans cells, the FOC, the COC, and the force fires center.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- (f) Planning, directing and supervising MEF liaison teams to external commands (e.g., the JTF, service and joint functional components headquarters, as appropriate) and intelligence organizations (theater, national, multinational).
- (g) Coordinating and supervising the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, in order to effectively support the MEF "single battle" transition process.

w Intelligence Operations Center. The IOC is the other principal MEF CE intelligence node. The three key subordinate elements within the IOC and their typical composition are the support cell, the SARC, and the P&A cell (see figure 5-8). It provides the facilities, CIS and other support to allow the ISC and intel bn to perform the following tasks:

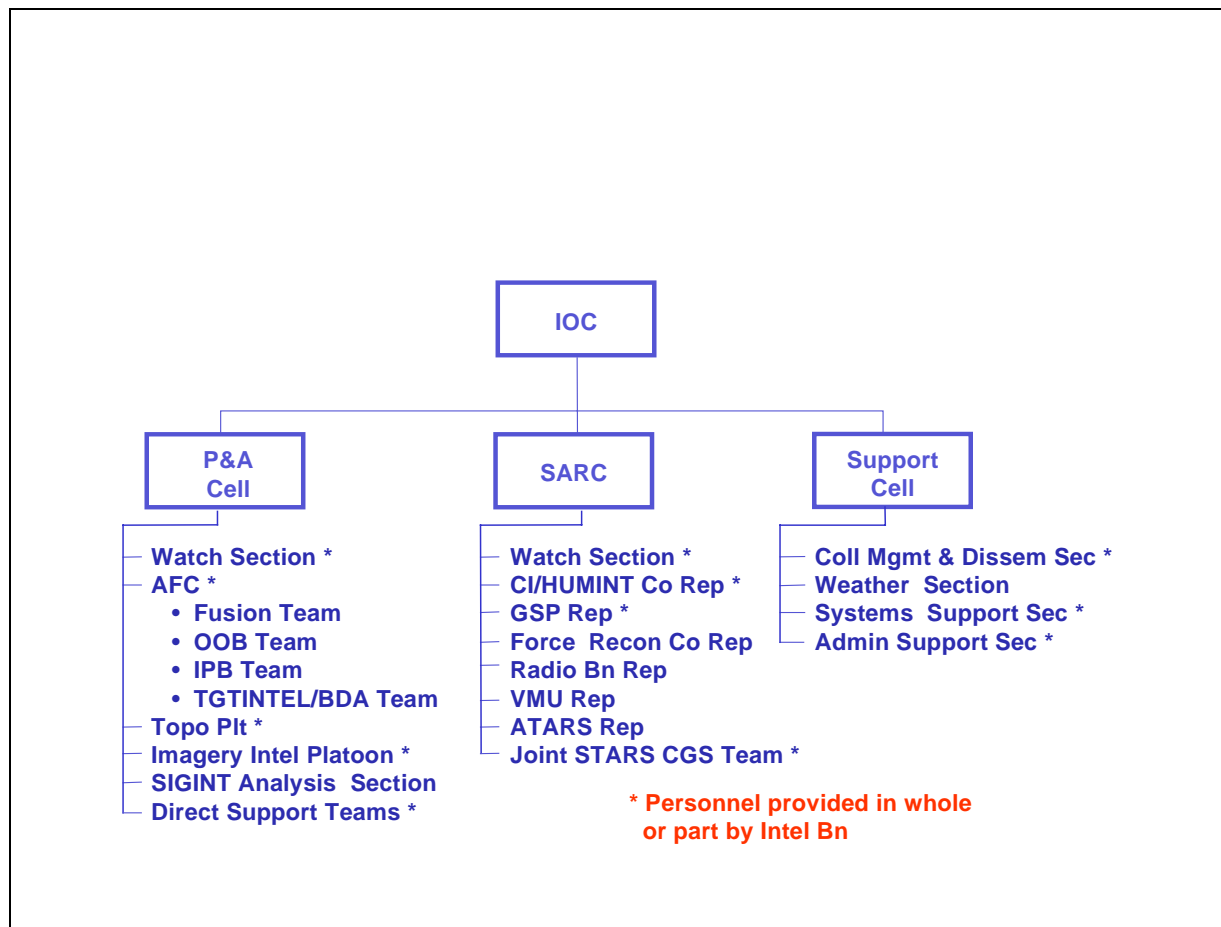


Figure 5-8. Intelligence Operations Center Elements and Composition

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 x Provide centralized direction for MEF intelligence operations under the staff cognizance
2 of the AC/S G-2. The IOC is the core for this task, with key assistance from the G-2 plans and
3 G-2 operations elements.
4

5 x Consistent with the commander's priorities, consolidate, validate, and prioritize IRs of the
6 entire force. The key CIC element providing for this is the CMD section within the IOC's
7 support cell. Intelligence specialists from all disciplines generally are organic to this section.
8

9 x Plan, develop, and direct the MEF collection, production, and dissemination plans and
10 operations. The key CIC elements providing for this are the CMD section within the IOC's
11 support cell and the P&A cell.
12

13 x Submit consolidated requests for external intelligence support through the Marine
14 component headquarters (or appropriate functional component headquarters if the JFC is
15 employing a functional C2 concept) to appropriate agencies. The key CIC element providing for
16 this is the CMD section within the IOC's support cell, with assistance from the P&A cell and the
17 G-2 operations branch.
18

19 x Allow the ISC to exercise, per AC/S G-2 cognizance, principal staff cognizance of MEF
20 organic and supporting intelligence, CI and reconnaissance operations, to include SIGINT,
21 IMINT, HUMINT, GEOINT, CI, MASINT, ground reconnaissance, and aerial reconnaissance
22 operations.
23

24 x Coordinate and manage the employment and reporting of MEF organic collection assets
25 through the IOC's SARC. Within the SARC will be representatives from most organic and
26 supporting intelligence and reconnaissance units to provide C2 and reporting of ongoing
27 intelligence operations.
28

29 x Maintain a consolidated, all-source intelligence production center in the MEF in the
30 IOC's P&A cell. The other nodes with significant intelligence production involvement are the
31 radio battalion's OCAC and the CI/HUMINT company's CP. Similar to the CMD section,
32 intelligence specialists from all intelligence disciplines generally are organic to the P&A cell.
33

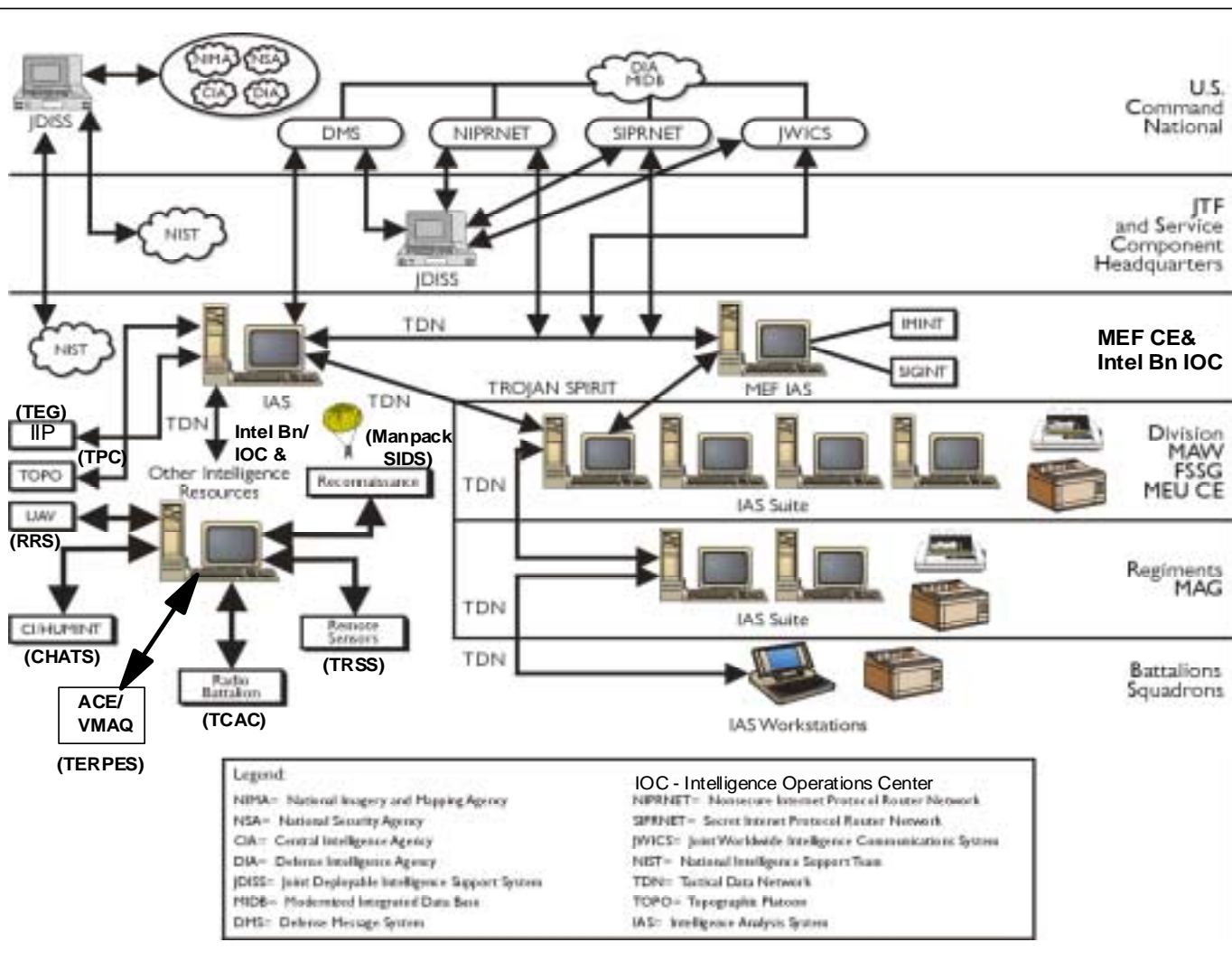
34 x Link the MEF CE to national, theater, joint, other-Service, and multinational intelligence
35 assets and operations. All intelligence intel bn and G-2 section nodes have common and unique
36 capabilities to perform critical tasks to accomplish this function. In addition to MEF CE
37 common communications pathways and TDN provided by the communications battalion, the
38 IOC generally will also have unique intelligence communications capability, such as Trojan
39 Spirit II.
40

41 w **CIS Support.** CIS support to CIC and IOC operations will vary from operation to
42 operation based upon METT-T. Generally all nodes will have or will have access to IAS and
43 JDISS (each with COLISEUM and other specialized applications) and connectivity with the full
44 range of communications (JWICS/SCI-TDN, SIPRNET/S-TDN, NIPRNET/U-TDN, DSN,

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

DMS, voice radio and telephone, video-teleconferencing, etc.) via either MEF CE common communications or unique intel bn CIS capabilities. Examples of unique intelligence CIS capabilities are those integral to the VMU squadron remote receive station (RRS), the radio battalion technical control and analysis center (TCAC) and the AN/MSC-63A special security communications central, the GSP's tactical remote sensor system, the IIP's tactical exploitation group (TEG), the VMAQ squadron's tactical electronic reconnaissance processing and evaluation system (TERPES), the CI/HUMINT automated tool set (CHATS), manpack secondary imagery dissemination (Manpack SIDS), Trojan Spirit II (TS-II), and the Joint STARS common ground station. See figure 5-9 for a depiction of a notional MEF overarching intelligence CIS architecture.

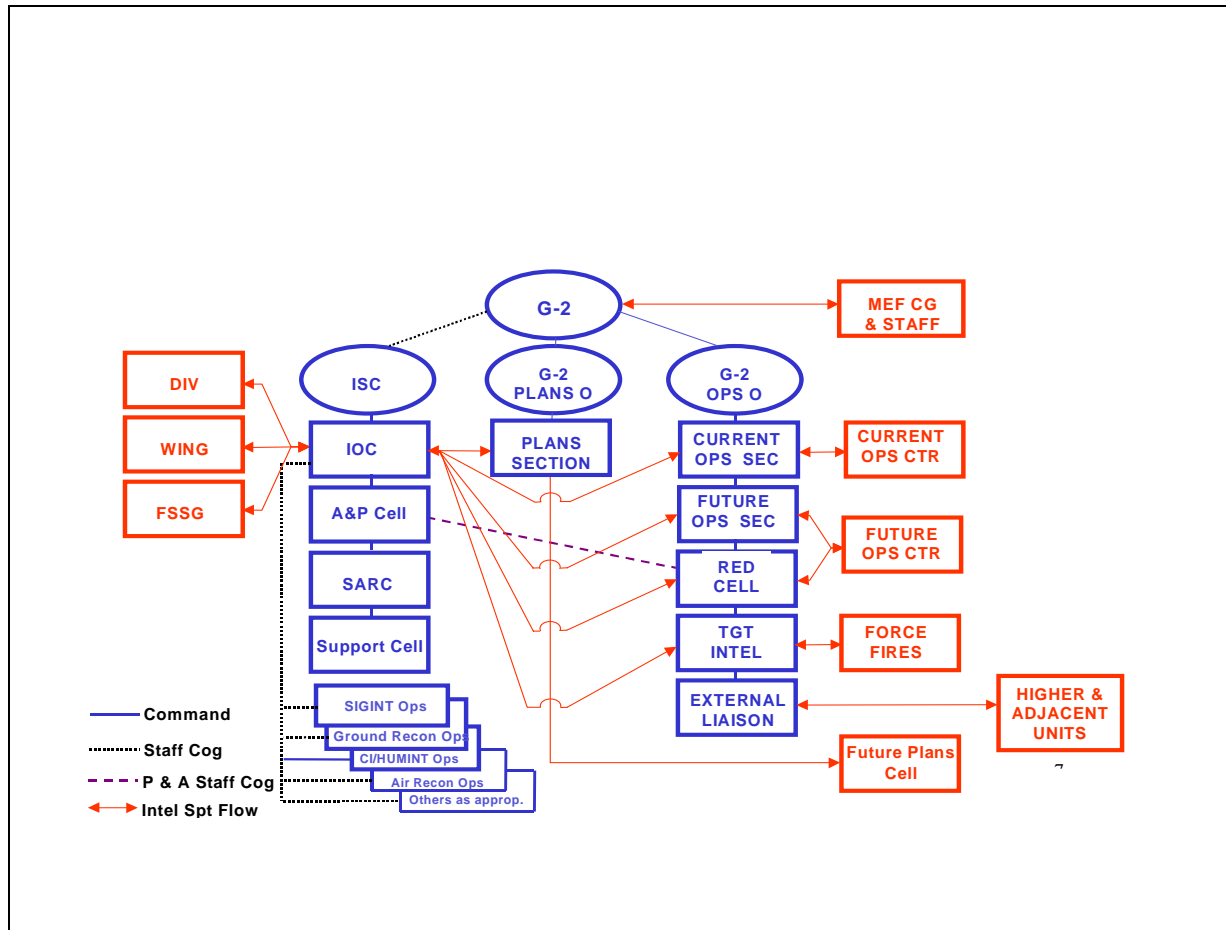


**Figure 5-9. Notional MEF Intelligence Communications and
Information Systems Architecture**

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

w The MEF G-2 section and intelligence battalion's overall command and control relationships and resulting all-source intelligence support flow throughout the MEF are as indicated in figure 5-10.



**Figure 5-10. MEF G-2 and Intelligence Battalion C2 Relationships
and MEF Intelligence Support Flow**

(2) MAGTF Subordinate Units' Intelligence Centers and Elements. IAS or the intelligence operations workstation (IOW) will be available at all command echelons down to the maneuver battalion/squadron levels. Communications connectivity between the MEF CE and its MSC HQs are predominantly provided by SATCOM, supplemented where practical with terrestrial line-of-sight and troposcatter multi-channel radio systems. Connectivity to the MSC HQs and down to the regiment/MAG level may be provided via U-TDN, S-TDN, SCI-TDN and various multichannel radio resources. Finally, communications connectivity below the regiment/group level depends principally on single channel radio primarily designed for voice traffic, with

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

limited range and limited data capacities (1.2 Kbps to 16 Kbps), secure telephones, and couriers. Although these units possess tactical data systems, their ability to exchange data traffic is currently limited due to the far less available bandwidth.

(3) Special Security Communications Elements and Teams. The mission of the special security communications elements and teams is to provide special intelligence (SI) communications support to the MAGTF. SI communications support for the MAGTF CE is provided by the special security communications element (SSCE) of the radio battalion. SI communications support for the division and MAW HQ is provided by special security communications teams (SSCT) -- small force units organic to each division and MAW. These teams operate under the staff cognizance of the AC/S, G-2/Special Security Officer. The special security element or team provides the personnel and equipment to install, operate, and maintain SI and SCI communications terminals. The communications circuits are provided by the communications unit supporting the HQ—the communications battalion for the MAGTF CE, the communications company for the division HQ, and the communications squadron for the MAW HQ. Close coordination is maintained by SSCE or SSCT with the supporting SYSCON and TECHCON to ensure adequate support and circuit priority. The special security elements/teams also may provide personnel augmentation to man ship's signals exploitation spaces (SSES) communications facilities as necessary to support landing force requirements. When done, those personnel consolidated will normally be with ATF special security communications personnel to operate on integrated ATF/LF special security communication center (SSCC).

5004. External Architectures. At the MEF CE level, the G-2 must maintain detailed information on the intelligence CIS systems and architectures of every theater combatant commander to which the MAGTF has contingency responsibilities, those of potential supporting national intelligence organizations, those of other U.S. military services' forces with which they may operate in a JTF and, as appropriate, those of allied/multinational countries' intelligence organizations.

5005. MAGTF CIS Architectures

a. Baseline Architectures. For each potential contingency, the intelligence officer must determine the architecture needed to provide the necessary intelligence support throughout the MAGTF and then develop the plans and conduct the training required to establish that architecture upon activation of the contingency. Since each contingency will have a specific mission, task organization, and unique operational environment, and each theater and JTF will have a mission-tailored intelligence architecture, MAGTF intelligence architecture planning must be both detailed and dynamic.

b. Tailored Architectures. Although baseline MAGTF CIS capabilities will provide the initial point of departure for intelligence architecture planning, changes will likely be needed to meet mission specific needs. Working closely with the MAGTF G/S-3, G/S-6 and G/S-1 (for messenger/courier service requirements), and higher, adjacent and subordinate intelligence officers, the MAGTF G/S-2 must plan and help prepare an internal intelligence CIS architecture that provides the MAGTF with access and interoperability with the broader intelligence system-

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 -in order to acquire needed tactical intelligence support for all MAGTF elements. Upon receipt
2 of a warning order or mission, the G/S-2 must (1) rapidly validate or update standing intelligence
3 CIS requirements; and (2) identify specific intelligence CIS priorities to support effective
4 collaborative planning.
5

6 **5006. Intelligence CIS Architecture Objectives and Planning Goals.** Intelligence CIS
7 architecture plans must reflect the broad range of potential missions and MAGTF task
8 organizations; the wide range of available communications, information and intelligence systems
9 in use today; and supporting organizational and functional SOPs to support all levels of the
10 MAGTF.
11

12 **a. The fundamental objectives of any CIS system** are equally applicable to intelligence CIS
13 architecture planning and development.
14

15 (1) The principle goal: allow rapid and comprehensive all-source intelligence fusion to
16 produce a picture of the battlespace intelligence that is accurate, available to all MAGTF
17 commanders and planners (as appropriate) in a timely manner and useable form, and satisfies
18 MAGTF tactical IRs.
19

20 (2) Support unity of effort, both within the MAGTF as well as the broader joint (to include
21 integration and interoperability with other services or functional components) and multinational
22 force.
23

24 (3) Exploit total force capabilities and support operational tempo through a responsive,
25 quickly installable, reliable and easily operated and maintained CIS system.
26

27 (4) Properly respond to and support the dissemination of time-sensitive intelligence to
28 commanders and other decisionmakers needing it.
29

30 **b. Additional intelligence CIS architecture planning goals include:**
31

32 (1) Early and continuous connectivity with JTF, theater, national, allied, naval and other
33 component intelligence, surveillance and reconnaissance organizations.
34

35 (2) Connectivity with tactical assets, to include combat and CSS units and all reconnaissance
36 and surveillance elements throughout the MAGTF in contact with the enemy.
37

38 (3) Phased expansion of tactical CIS capabilities in support of all MAGTF forces
39 commencing with the initial contingency alert/planning, during the subsequent deployment and
40 movement phase, and on through rapid establishment of full capabilities upon arrival within the
41 AO and subsequent operations.
42

43 (4) Establishment of an internal MAGTF intelligence architecture that supports the six
44 principal intelligence functions.
45

(5) Determination of unique CIS architecture requirements for each intelligence discipline (i.e., SIGINT, CI, HUMINT, IMINT, MASINT, GEOINT, OSINT, ground and air reconnaissance, etc.).

(6) Standardization of intelligence methods, modes, databases, product formats, procedures and other relevant intelligence CIS functional activities.

5007. Intelligence CIS Architecture Planning Methodology. The following intelligence CIS planning methodology (see figure 5-11) provides a simple framework for intelligence CIS architecture contingency preparations and peacetime training opportunities. As with the intelligence cycle, this intelligence CIS planning methodology is not a purely sequential process. Rather, it is a dynamic process that seeks to anticipate and plan for future CIS requirements while concurrently adjusting to current operational and tactical circumstances.

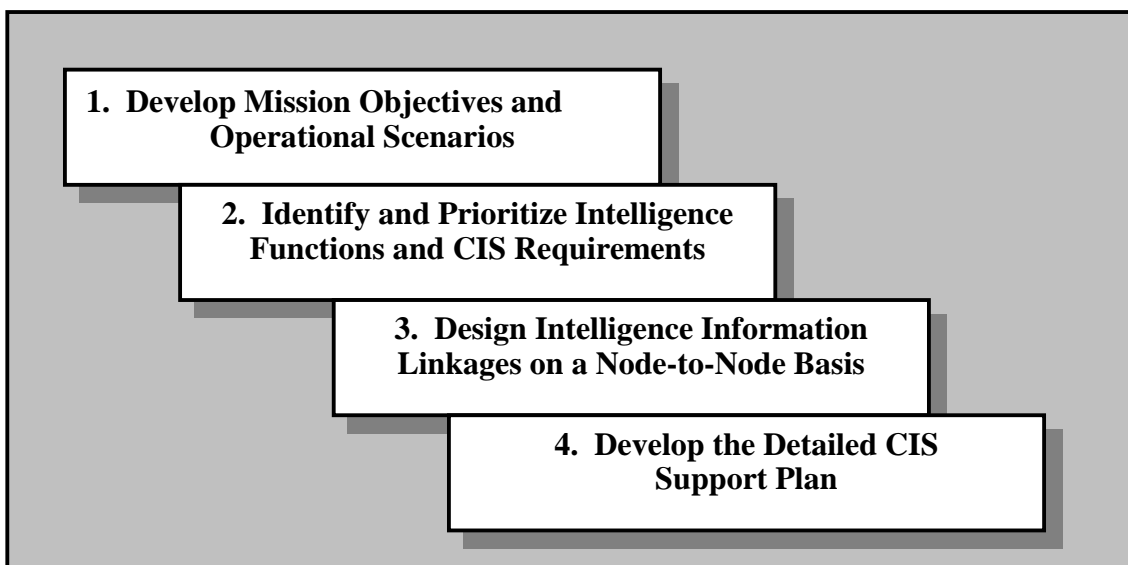


Figure 5-11. MAGTF Intelligence CIS Planning Methodology

a. Step 1 -- Develop Command, CIS and Intelligence Mission Objectives and Operational Scenarios. During this step, intelligence planners endeavor to clarify, specify and assess command missions, supporting objectives and tasks, and preliminary multi-functional concepts of operations in order to establish the broad intelligence CIS architecture needs. Key information to consider includes:

(1) Multi-echelon commanders' intents, situational assessments, concepts of operations and their desired endstates, initial planning guidance and PIRs/IRs.

(2) MAGTF, JTF, and other forces committed to or supporting the operation, with special attention to available intelligence reconnaissance and CIS resources (personnel and equipment).

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(3) Command relationships, with special attention to ownership and tasking authority of supporting CIS and intelligence collection, production and dissemination resources.

(4) Estimated planning and execution timelines, focusing on operational phases.

(5) Characteristics of the operating area, the nature and capabilities of the threat, and the nature and capabilities of other significant political, military, economic and sociological players in order to identify early PIRs and other unique factors which may influence CIS architecture development.

(6) Early anticipated MAGTF operational activities -- such as the deployment of an alert contingency force, a special-purpose MAGTF (SPMAGTF) or lead echelon of the MEF -- and associated intelligence needs.

b. Step 2 -- Identify and Prioritize Intelligence Functions Required to Support the Operations Plan, Intelligence Flow and Associated CIS Needs. The nature of the mission (conventional combat, disaster relief, NEO), the information acquired in step 1, already available intelligence, available time and the JTF/Components'/MAGTF's (and subordinate elements') operational, CIS and intelligence concepts of operations will provide the minimum information required for this step. The endstate is a clear listing and prioritization of intelligence CIS requirements. The intelligence officer must continually assess and determine the relative priorities among the six basic intelligence functions and ensure that the most critical priorities receive essential CIS support until conditions allow for the establishment (or restoration) of full JTF and MAGTF CIS capabilities. The intelligence concept of operations and functional priorities determined by the MAGTF intelligence officer will set the direction for subsequent intelligence CIS planning.

c. Step 3 -- Design Intelligence Information Linkages on a Node-to-Node Basis. This step compiles all acquired information into a node-to-node depiction of intelligence C2, information management, and CIS activity. Nodes are used to represent headquarters (or more specifically, intelligence, C2, fires and other elements within a HQ, such as the IOC or the COC) and external supported/supporting organizations. Connectivity requirements, sometimes called *needlines*, between nodes will identify as appropriate the intelligence function(s) they serve, specific associated intelligence and communications systems, an estimate of communication volume and priority, and essential technical characteristics associated with the needline.

(1) For planning purposes, a useful technique to use when depicting the MAGTF's intelligence CIS architecture is to break it down into two distinct elements.

-- That portion which depicts the command and key staff CIS nodal linkages among principal warfighting units or their C2 nodes (e.g., from the MEF Command element G-2 to the JTF J-2 and Marine Division HQ G-2).

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

-- That portion which depicts nodal linkages among intelligence and reconnaissance units and specific command posts (e.g., from deployed ground reconnaissance or Joint STARS aircraft and the SARC).

(2) Upon completion of this step, MAGTF intelligence CIS planners – principally intelligence battalion's CMDO -- will provide to the MAGTF G/S-6 (and the G/S-1 for courier requirements) the prioritized listing of intelligence CIS requirements. Copies should likewise be provided to the MAGTF G/S-3 and to higher and subordinate units' intelligence officers (and other intelligence planners, as required) to support concurrent multi-echelon intelligence CIS architecture development. The G/S-6 will then coordinate the CIS plan to satisfy these requirements consistent with the commander's overall operational, C2 and CIS priorities.

(3) When stating requirements to CIS planners, intelligence planners' focus should be on the intelligence function and associated unique technical and operational requirements in order to allow the G/S-6 maximum flexibility regarding how to satisfy the requirement. The following information, at a minimum, must be specified.

-- **Intelligence CIS Requirement** -- statement regarding the intelligence function/role to be performed -- for the G/S-2 section, intelligence battalion and of organic and supporting intelligence and reconnaissance units. Initially, each intelligence CIS requirement should be separately stated. Subsequent G-6/G-2 CIS planning will determine if an option will support multiple requirements (e.g., an option may support both intelligence dissemination and C2, vice being dedicated to one or the other).

- Priority -- relative priority vis-a-vis other intelligence CIS requirements.
- Link/net subscriber composition -- listing of commands and/or intelligence organizations that will be participants/users.

-- **Operational requirements** -- these should address operational factors that add focus to each requirement. Operationally oriented information that may be useful includes:

- Date/time for initial activation of the requirement.
- Physical location of command posts or intelligence units.
- Necessary placement within an intelligence C2 node of certain CIS terminals.
- Whether the requirement is necessary for all or select phases of an operation.
- Whether the needline is required for 24-hour continuous usage or as required availability.
- Whether there is a requirement for access to restricted or special security communications (e.g., RODKA, SCI).
- Whether inclusion of the units on distribution for additional address indicator groups (AIGs), collective address disgnators (CADs) and DSSCS address groups (DAGs) is needed.
- Whether requirement is necessary during intelligence C2 node displacements and, if so, identifying with what intelligence C2 node/echelon each is

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

associated and any acceptable modifications to routine operating characteristics.

- Standard message/reports formats.
- Distribution of messages, to include to whom and quantity: record, automated, manual.
- Type of dissemination channel and mode desired.

-- **Technical requirements** -- these should address any unique technical factors that have bearing on the requirement's satisfaction. Technical information that may be pertinent includes:

- Type service required (e.g., data, voice, video, LAN, WAN, facsimile, etc.).
- Type operation (e.g., full duplex, multi-point receive only, etc.).
- Estimates of link usage activity or volume (for both routine and surge operations).
- Recommended circuits and systems restoration priorities.
- Minimum security classification and any special handling considerations for information to be processed/transmitted.
- Message formats and reports to be processed.
- Wide and local area network requirements: use of homepages, server requirements, IP addresses, etc. Generally this should clearly differentiate between WANs and LANs internal and external to the MAGTF.
- Systems administration procedures, database access & types, database maintenance, etc.
- Precedence levels (flash, immediate, priority, routine).
- Specific minimum speed of circuit requirements: number of channels, bandwidth, rates.
- Frequency ranges of organic equipment.
- Routing indicators (for SCI communications only).
- Whether additional off-line peripheral equipment, unique software applications, or special personnel expertise is needed.
- Power outputs and available antenna support.
- Details regarding telecommunication service request preparations (SCI CIS requirements only).
- Known unique cryptographic requirements and account codes.
- Known unique tempest requirements.
- Desired quantity of terminal drops (e.g., for telephone and LAN stations within an intelligence C2 node) and recommended drop names (e.g., the name of the telephone's primary user, or the preferred e-mail account name for the LAN station).

d. Step 4 -- Develop the Detailed CIS Support Plan. Effectively developing this plan -- and its supporting branch plans -- is a true multi-echelon, J/G/S-2/6/3 effort. The CIS officer's focus is on providing the necessary communication channels, interfaces and media necessary to

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

move intelligence throughout the MAGTF, and to lateral elements and higher echelons. The intelligence officer remains focused on the employment of allocated and other available CIS resources in performance of the MAGTF's current and anticipated future intelligence missions. Additionally, the G/S-2 must maintain close coordination with J/G/S-3s regarding current and future operational missions and requirements.

5008. Basic Standing Intelligence CIS Requirements. Regardless of the size of the MAGTF, there are certain standing intelligence CIS requirements which must be satisfied. These requirements are:

a. Ability to Command and Control Subordinate Units. Intelligence officers and intelligence and reconnaissance unit commanders/OICs must be capable of positive C2 of subordinate units and organic/attached intelligence elements, and the integration of their operations with broader MAGTF and external intelligence and operations C2. Traditionally single-channel radio (SCR) and record message traffic have been used to support C2 of MAGTF intelligence units. In semi-static situations, secure e-mail via WANs/LANs or telephone may be the method of choice, while in highly fluid or mobile scenarios, cellular, SATCOM, and VHF and HF radio may be used.

b. Ability to Receive and Transmit Collected Data and Information from Collection and Deployed Elements. The MAGTF intelligence CIS architecture must provide connectivity between organic and supporting collection or deployed elements (such as the HUMINT support teams, SIGINT collection or DF teams, the Tactical Exploitation Group (TEG), GEOINT support teams (GISTs), and reconnaissance elements); IMINT (IIP), GEOINT (Topo Platoon), SIGINT (RadBn OCAC and VMAQ TERPES), CI/HUMINT Co. CP) analysis and production centers, and supported MAGTF operations and intelligence centers (P&A Cell, COC, FOC, FFC). Requirements include the access to high capacity JWICS, SIPRNET, and NIPRNET networks for external communication and SCI tactical data network (SCI-TDN), SECRET TDN (S-TDN), and unclassified TDN (U-TDN) for internal MAGTF communications, as well as the capability to transmit collection files and reports digitally via fiber-optics, wire, or radio/telephone in formats (both voice and data) that are readily usable by the analysts and in a format allowing rapid dissemination.

c. Ability to Receive and Disseminate Indications and Warnings. I&W intelligence is disseminated in a variety of means to include voice, record messages, tactical reports, e-mail, and intelligence broadcasts. Having the capability to receive the information, recognizing the I&W intelligence as such, and possessing a C2 and CIS method to disseminate this I&W intelligence to the affected units and decisionmakers are key to satisfying this requirement.

d. Ability to Provide Intelligence to Supported Commanders. The required intelligence CIS architecture must support the commander's (and subordinate commanders') intent, concepts of operations and intelligence, command relationships, and standing PIRs and IRs. The MAGTF intelligence architecture must be capable of integrating CI/HUMINT, IMINT, SIGINT, GEOINT, and reconnaissance element C2 and supporting CIS operations (to include special communications capabilities and channels unique to intelligence reporting) with the primary CIS channels used by supported commanders for MAGTF C2. Such CIS requirements must support

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

both push and pull capabilities. Push capabilities are needed so that topographic and other intelligence elements can send updated files and products to MAGTF command echelons or specialized distributions. Pull capabilities are needed so that commanders, planners and intelligence personnel at all MAGTF echelons can access, review, and retrieve data files, reports and other products pertinent to their intelligence needs.

e. Ability to Share Intelligence Products and Reports. The MAGTF intelligence CIS architecture must provide the means to share products and reports from the various intelligence disciplines with MAGTF intelligence elements and all-source production centers, and with specialized and all-source JTF, components, theater, and national intelligence centers. The traditional means for providing this capability are MAGTF GENSER secure record and voice communications, the SCI-secure Defense Special Security Communications System (DSSCS) for record communications, and operator's communications (OPSCOM) circuits for SIGINT analyst-to-analyst exchanges and coordination. While these techniques continue to be used at the MEF and MSC levels, they are rapidly becoming secondary in importance to the use of JWICS, the SIPRNET, and specialized CIS capabilities (such as NSA NET) which allow participants to access each others unique products and databases and to immediately pull required intelligence data and products. Similar capabilities exist within the MAGTF with SCI-TDN, S-TDN employed with intelligence systems such as IAS, TCAC (technical control and analysis center), TEG, TPC (topographic production capability) and CHATS (CI/HUMINT automated tool set). It is important to note that at the lower tactical levels, the ability to operate a WAN is limited when regiments, battalions, etc. are engaged or on the move. Therefore, the ability to transition the dissemination of critical intelligence from automated data processing (ADP) systems to single channel radio or other means is vital.

f. Ability to Receive Intelligence Broadcasts. Broadcast receivers currently being fielded and under development will allow MAGTFs to receive multiple channels of JTF, fleet, theater, and national intelligence broadcast data. This data includes all-source intelligence, SIGINT and IMINT on enemy operations as well as friendly positional and other information. Effective planning, design, and integration of SCI and GENSER CIS and proper information filtering, correlating, and tailoring prior to dissemination or display is necessary to provide timely reporting to supported commanders while preventing information overload.

5009. MAGTF Dissemination SOPs, Plans and Orders

a. Responsibilities. The AC/S G-2 has overall responsibility for MAGTF intelligence dissemination SOPs, plans and orders. The ISC is responsible for the preparation of the intelligence dissemination plan and the intelligence CIS plan, with his CMDO executing this authority.

b. OPLAN/OPORD Background. The principal intelligence CIS planning guide/tool for a MAGTF operation is Tab D, Intelligence CIS Plan, to Appendix 16 (Intelligence Operations Plan) of an OPLAN/OPORD's Annex B. Most other portions of Annex B, however, will likewise include key intelligence CIS information, particularly: Tabs A, B, and C to Appendix 16

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(respectively, the collections, production and dissemination plans); Tab E (Intelligence Reports) to Appendix 16; and Paragraph 5 (Intelligence C2) to the basic Annex B.

Besides the Annex B, there are key portions of Annex K (CIS) that will be significantly influenced by intelligence CIS architecture planning. These include:

- Appendix 14, Communications Restoration
- Appendix 23, Task Organization/Communications Guard Shifts
- Appendix 26, Radio Battalion/SSO Communications
- Appendix 31, Communications Support for Intelligence
- Appendix 34, IP Assignments
- Appendix 35, CIS Support for Information Management

c. Standing Operating Procedures. Although there is no established format for an SOP, one of two formats is generally used. An SOP may be formatted as an all-inclusive document containing in the main body sections and paragraphs detailing the duties and responsibilities of subordinate units and, where applicable, of personnel. This format does not have annexes or enclosures. The other approach is to publish the main body of the SOP as a basic document containing instructions of a general nature with annexes for technical details and specific instructions for individual units and/or personnel. For example, the basic document could contain information for the communications battalion as a whole with annexes for different functional areas such as TECHCON and systems planning and engineering. SOPs prepared by subordinate units must comply with and be coordinated with pertinent parts of the SOP of the higher command. SOPs should not repeat practices of procedures governed by other directives or documents that are readily available to all elements of the command unless such repetition is required to clarify local operating practices. Suggested content:

- References (such as MCWPs, field manuals, technical manuals, regulations, and the SOPs of higher commands).
- Planning checklists.
- Training instructions outlining general training standards. Detailed instructions are normally contained in quarterly training schedules.
- Information systems security instructions that address both COMSEC and computer security. Instructions should be limited to those that are applicable to all elements of the command and are not contained in the command CEOI, as the purpose of this section should be to develop and maintain CIS security awareness throughout the unit.
- Physical security instructions designed to develop an awareness for physical security and to promulgate and standardize physical security procedures throughout the unit.
- Instructions for the operation of communications centers, including location and procedures for transmittal, receipt, and processing of record traffic.
- Procedures covering the exchange of organizational and individual e-mail. The authorization for use and the records to be maintained should be prescribed.
- Directory service information, guidance for obtaining communication service, and instructions for maintenance of equipment and lines should be considered.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

- Instructions pertaining to the planning, installation, operation, and maintenance of SCR equipment, and guidance for the composition and operation of intelligence radio nets.
- Instructions on procedures to be employed by all users for the dissemination of time-sensitive intelligence and the use of alternate means of dissemination
- General procedures to be employed by all users for the planning, installation, operation, and maintenance of intelligence and SCI facilities.

d. Intelligence CIS Concept. After developing the CIS estimate and gaining the commander's approval, the CIS officer prepares the CIS concept. The concept outlines how CIS are to be employed to support command and control throughout the operation. The CIS concept includes information such as:

- Numbers, types, classification levels, and locations of intelligence C2 facilities.
- Numbers, types, classification levels, locations, and mode of operation of intelligence SCR nets.
- Numbers, types, classification levels, locations, and channelization of intelligence multi-channel radio circuits, including location of transmission equipment.
- Numbers, types, classification levels, and locations of intelligence-related wire circuits, including location of terminal equipment.
- Numbers, types, classification levels, and locations of intelligence-related radio-wire integration facilities.
- Numbers, types, classification levels, and locations of intelligence-related LANs.
- Numbers, types, classification levels, and locations of switching centers, routers, and gateways.
- Numbers, types, classification levels, locations, and channelization of intelligence-related satellite links, including location of intelligence CIS terminal equipment.
- Numbers, types, classification levels, and locations of terminal devices (computer, facsimile, etc.).
- Frequency requirements.
- Call sign requirements.
- Visual, sound, and messenger communications.
- Communication control procedures, including number, types, and location of communications control facilities.

The above list is not all-inclusive. It provides general guidance for preparing the CIS concept. Concept development should be closely coordinated with OPLAN/OPORD development. The concept is modified and refined as necessary and then promulgated as Annex K to the OPLAN/OPORD.

e. Tab C (Intelligence Dissemination Plan) to Appendix 16 (Intelligence Operations Plan) to an Annex B of an OPLAN or OPORD. Annex K of this publication provides an example format of an intelligence dissemination plan. Additionally:

- This is the principal intelligence dissemination planning guide/tool for an actual operation.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- Its purpose is to explain how intelligence dissemination elements under the command or supporting the MAGTF will be used to support intelligence dissemination operations.
- An intelligence dissemination plan will generally be produced by the MEF and MSC G-2s, and may be prepared by other subordinate S-2s.
- While it is focused on dissemination, the intelligence dissemination plan must be well-integrated with the collection and production plans.

f. Tab D (Intelligence Communications and Information Systems Plan) to Appendix 16 (Intelligence Operations Plan) to an Annex B of an OPLAN or OPORD. Annex G of this publication provides an example format of an intelligence CIS plan, which should include architecture graphics in the tabs. The intelligence CIS plan should accomplish three purposes:

(1) Provide necessary text and graphics to identify CIS plan for each intelligence & reconnaissance discipline – SIGINT, IMINT, CI, HUMINT, GEOINT, Remote Sensors, Ground Recon, and Air Recon. This will clearly identify how intelligence C2 over these operations is supported via CIS, and how these disciplines' collection, reporting and production is supported by CIS.

(2) Provide an integrated, overarching unit intel CIS picture. This is especially valuable for commanders, planners, and key watch personnel in places like the COC, FOC and FFC, as these are the CIS means they will get most of their intelligence support via.

3) Provide a detailed CIS plan/graphic showing key intelligence systems and supporting communications pipes/terminal capabilities within a command post or, especially in the case of large intel ops, key intel C2/ops nodes (e.g., the Support Cell, the SARC, the P&A Cell, & the intelligence section watches in the COC, FOC and FFC). This will mostly be intelligence systems, networks (S-TDN) and big pipes, but also at least an identification of generically typical single channel radio nets in places like the SARC, OCAC, COC, etc. Additionally:

- This is the principal intelligence CIS planning guide/tool for an actual operation. Its purpose is to explain how intelligence-related CIS under the command or supporting the MAGTF will be used to support intelligence dissemination operations.
- An intelligence CIS plan will generally be produced by the MEF and MSC G-2s, and may be prepared by other subordinate S-2s.
- There is no standard format for the intelligence CIS plan; however, it must reflect unit SOP, METT-T factors, and the complexity of the unit's C2/intelligence/CIS operations.
- In most cases, a graphical depiction of the intelligence CIS plan/architecture is recommended and may be sufficient to support planning.
- While it is focused on dissemination, the intelligence CIS plan must be well-integrated with the collection and production plans.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

g. Tab E (Intelligence Reports) to Appendix 16 (Intelligence Operations Plan) to an Annex B of an OPLAN or OPORD

- Specified formats for all intelligence reports will be identified here in Annex B.
- The CMDO is responsible for this tab to appendix 16; however, he must closely coordinate with the P&A Cell OIC, SARC OIC, and all intelligence and reconnaissance unit commanders/OICs to ensure its accuracy, sufficiency, and understanding.
- Normally, only changes from unit SOPs will be identified and laid out here. However, if significant global sourcing of units occurs, or if the Marine unit will have either attached or in direct support any joint or other services' intelligence/reconnaissance elements, then the appendix will normally be included and will identify ALL intelligence reports formats to be used.

Chapter 6

Intelligence Estimates and Studies

6001. Overview. Intelligence estimates, studies, reports, and briefings, the principal intelligence products disseminated during MAGTF operations, are discussed within the context of dissemination in chapters 6, 7, and 8 of this publication. Detailed information on preparing each of the above is contained in MCWP 2-12, *MAGTF Intelligence Analysis and Production*, and other intelligence series MCWPs.

Whether oral, text, or graphic, intelligence products should use standard formats whenever possible. Standard formats facilitate ease of preparation and dissemination, as well as usability of the intelligence product. The basic intelligence products used in MAGTFs (e.g., IPB templates and matrices, intelligence estimates, summaries, reports, and briefings) have baseline formats. Individual units may modify formats to suit METT-T factors, but modifications may have an impact on interoperability within and external to the MAGTF -- and thus must be thoroughly coordinated with all. The bottom line is that intelligence must be presented so that all supported commanders and other decisionmakers truly understand its significance in terms of effects on the battlespace and on friendly and threat military operations.

6002. Intelligence Estimates and Studies

a. Purpose. The purpose of disseminating intelligence estimates and studies is to provide large amounts of detailed data in support of general operational planning. Although most estimates and studies are normally scheduled production documents--especially at national-level agencies and senior-level military commands--certain indepth estimates and studies must be produced and distributed quickly if a rapidly developing crisis may lead to commitment of a MAGTF.

b. Dissemination Considerations. Due to their detail, composition and size, the most efficient means of distributing intelligence estimates and studies to a wide audience usually is via hardcopy, floppy disk, and CD-ROM mail-out to a predetermined distribution list or softcopy transmittal via a secure datalink. In most cases, broader dissemination will be possible by posting these products on homepages accessible via S-TDN, SCI-TDN, SIPRNET and/or JWICS.

c. Advantages. Intelligence estimates and studies provide consumers with large quantities of intelligence and information--often complete with overlays, color graphics and other aids -- in a standardized format. Once disseminated, the documents are available for continuous reference by intelligence staffs. Users can select and utilize those portions that apply to specific command requirements.

d. Disadvantages. While intelligence estimates and studies can serve as invaluable background references, they require significant time and resources to produce. Also, all such products are

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

prepared with a specific information or intelligence cut-off time, and once written, they are difficult to update quickly. In a crisis situation, intelligence estimates and studies are cumbersome to reproduce mechanically for rapid dissemination to all necessary subordinate units. Finally, reproduction or reformatting of imagery and geospatial information materials can be particularly cumbersome.

6003. Types

a. Intelligence Estimate

(1) Description. The intelligence estimate is the primary means for providing basic and current intelligence and results of the IPB effort focused on a specific mission. It is usually the first significant intelligence product developed to support initial orientation, immediate mission analysis and other planning needs. An intelligence estimate can be prepared at any level, from the battalion/squadron through the MEF command element and MARFOR headquarters levels, and should usually be disseminated at least two echelons higher and lower than the originating command. The scope and detail of the estimate will be governed by the level of command preparing it, the nature of the operation it is intended to support, already available intelligence, identified IRs, prior contingency planning, and the time and resources available. The intelligence estimate should be succinct, yet provide commanders and staffs the necessary intelligence for planning and early decisionmaking. Serving as a summary of basic intelligence, the estimate normally uses supporting studies for indepth treatment of specific aspects of the enemy situation or the area of operations. When contained in an OPLAN or OPORD, the intelligence estimate will be Appendix 11 to Annex B.

(2) Format. Whenever possible, the intelligence estimate should clearly present the analysis and conclusions developed during IPB. The finished estimate may be written, graphic, or verbal in form, but should follow the general five paragraph format shown in Appendix C. Subparagraphs and tabs may be added and omitted as necessary, based on their relevance to the stated mission. For topics that require a large amount of data, information and intelligence (i.e. beaches, weapons capabilities and technical characteristics, etc.), the salient facts and conclusions should be summarized in the body of the estimate with details included as a tab(s).

b. MAGTF Contingency Intelligence Study. This is a baseline intelligence study prepared in advance for standing OPLANs and likely contingencies. In written form, it is based on the intelligence estimate format and can be relatively quickly updated and converted into an intelligence estimate when an alert or warning order is received. Many of the products produced in the IPB process can be prepared either as supporting graphics or as stand-alone products. The format can be modified to suit the user, or METT-T, especially for military operations other than war (MOOTW).

c. Intelligence Studies. Intelligence studies deliver detailed intelligence on specific aspects of the AO or threat--such as enemy beaches, minefields, HLZs, hydrography, or airfields. As indepth examinations of specific items of interest, studies directly support intelligence estimates. Wherever possible, standardized formats should be used, and essential intelligence should be

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

transformed into graphics. Unit intelligence studies should be disseminated at least two echelons upward and downward, especially if the intelligence contained in the study is derived from organic collection assets.

d. IPB Products. IPB is a continuous, systemic process of analyzing the threat and environment presented in the intelligence estimate. These provide supported commanders and planners with a graphic portrayal of the battlespace. By integrating, analyzing, evaluating, interpreting and fusing vast amounts of textual information into symbols, IPB products convey easily-understood "snapshots" to operators and planners – but always with detailed supporting intelligence available in supporting text products or intelligence databases. Overlays, such as MCOO, LOC and fields of fire overlays, quickly and effectively depict such key terrain and enemy characteristics as mobility corridors, obstacles, terrain trafficability, and threat courses of action (COAs). While IPB products can be developed independently, most are initiated as part of the intelligence estimate process in the planning phase. IPB overlay updates should always be disseminated as rapidly as possible to other staff sections and subordinate units. Standardized formats for IPB products should be used to the maximum extent possible (see MCWP 2-12, *MAGTF Intelligence Analysis and Production*; MCWP 2-12.1, *Geographic Intelligence*; and MCRP 2-12A/FM 34-130, *Intelligence Preparation of the Battlespace [draft]*), tailoring as appropriate according to the situation or a user's unique needs.

e. Target/Objective Studies

(1) Purpose. Target/ objective studies are focused, detailed intelligence products which aid in the application of fires or the maneuver of forces against a specific target set or area. These studies can also be utilized by small units, such as MEU(SOC)s, for mission preparation and execution. IPB impacts development through the evaluation of terrain and weather, and the association of threat forces at specific times and locations within the battlespace. Situation, event, and decision support templates identify named areas of interest (NAIs). Once identified, NAIs can then confirm or deny a threat's activities or adoption of a particular COA. Additionally, decision points and target areas of interest (TAIs) are identified which require key intelligence that supports either fire or maneuver. From the IPB and wargaming processes, HVTs and HPTs are derived.

(2) Content. Target/objective studies are graphically oriented and may utilize many of the graphics derived during the IPB process. One such product is a target folder, which contains the following information depending on the specific mission:

- * Orientation Graphic

- * Time-Distance Graphic

- * Weather Forecast

- * Hydrographic Forecast and Astronomical Data

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

* Intelligence Briefing Notes For Mission

* Graphic Intelligence Summary

* Objective Area Graphic Enhancements

-- Orientation Graphic (10-20 KM around Objective)

-- Mission Planning Graphic (5 KM around Objective)

-- Objective Area Graphics

-- Objective Area Imagery

* Imagery and Graphics of Insertion Points

* Survival, Evasion, Resistance, and Escape (SERE) Plan

* Challenge and Password

* Mission Specific Data as Required

(3) Forms and Uses. This intelligence product is used to provide basic tailored, detailed, mission-specific intelligence in support of small unit execution. There is one basic form, but many variations can be used. Usually, it consists of both text descriptions supported by graphics. Graphics are the main part -- annotated imagery, map enhancements, terrain models, blueprints/diagrams/schematics. Target folders consist of intelligence required to engage or operate against a particular target and are most often utilized by aviation or artillery units, MEU(SOCs), and raid forces. It can also be used to support regular combat operations (e.g. a rifle company attacking or defending a hill). Although containing both textual descriptions and graphics, target folders are most useful to operators if constructed primarily with annotated imagery, map enhancements, diagrams, schematics, and mapping products. In a tactical situation, target intelligence becomes highly perishable and must be disseminated as quickly as possible to controlling, coordinating, and delivering units.

f. Other Typical Study Products. A wide range of other studies are typically used by Marines. The below identifies the most common. See the associated MCWP for additional information on each.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

Publication	Title	Type of Study
MCWP 2-12	MAGTF Analysis and Production	MCOO
MCWP 2-12.1	Geographic Intelligence	Tactical Study of the Terrain
MCWP 2-14	Counterintelligence	Various counter-HUMINT, counter-SIGINT, and counter-IMINT products
MCWP 2-15.2	Signals Intelligence	SIGINT Product Reports
MCWP 2-15.4	Imagery Intelligence	Target folders Beach studies HLZ and DZ Studies Airfields and Ports Studies

6004. Preparation Principles. In preparing intelligence estimates and studies, very close coordination is needed between production and dissemination leaders and all supported intelligence officers. Dissemination methods and means available to subordinate units must be considered in order to allow for maximum and rapid distribution of products throughout the MAGTF. To enhance effective dissemination:

- **State requirements clearly** -- so that intelligence production and resulting products will meet needs without being reformatted and can most effectively be disseminated to all requiring these. IPR identification also should include anticipated needs and times for updates to disseminated estimates and studies.
- **Always clearly identify the information/intelligence cut-off time** used in a product's development.
- **Use standardized formats** -- to the maximum extent possible.
- **Coordinate dissemination planning among all echelons** -- but be aware of reproduction limitations and time delays -- to include those of subordinate units which may have need to further disseminate the intelligence to their subordinates.
- **Use executive summaries technique.** In assembling estimates and studies for dissemination, intelligence personnel should always summarize key intelligence findings and assessments from the body of the document in an executive summary format. Indeed, in crisis situations, the executive summary may be the only part of an estimate or study that can be disseminated quickly enough to support tactical commanders. Supplemental detailed information can then be attached as appendices or supporting studies, or if the MAGTF TDN can support it, via intelligence homepages or accessible intelligence databases.
- **Use graphics.** Graphics should be used wherever possible, keeping in mind that certain units

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

may have limitations in display and reproduction technologies. For example, colored graphics do not reproduce well in black-and-white if symbology is not obvious in the absence of color.

- **Cross-check for clarity.** All numerical data should be carefully cross-checked for accuracy, especially quantities of enemy units/resources and map coordinates. If place names--especially those written in native languages--are mentioned in text, they should always be shown on corresponding graphics for clarity.
- **Use standardized units of measure** -- understandable by both U.S. and allied forces. Each estimate or study should employ standardized units of measure to avoid confusion.
- **Provide linkage to supporting intelligence.** Disseminated intelligence estimates and studies should include clear identification to other intelligence reports, products and databases that provide detailed intelligence in support of the basic estimate or study. If these are accessible via automated means, then pertinent information should be provided. If not, then include information for how these may be obtained (unit/cell name, POC, telephone number, e-mail address, etc.).

Chapter 7

Intelligence Briefings

7001. General. Intelligence personnel at all command levels will frequently use intelligence briefings – formal and informal – to disseminate intelligence to commanders, staffs and others. The ability to prepare and orally convey relevant intelligence in a clear, concise manner is an essential skill for intelligence personnel.

7002. Purpose. Intelligence briefings are used to convey specific intelligence and intelligence operations details to a selected audience in a concise, mission-oriented format. Depending on available preparation time, briefing styles can range from formal presentations with detailed hand-outs and graphics to strictly oral updates. Even in the absence of formal tasking to prepare an intelligence briefing, intelligence personnel will informally disseminate intelligence at every opportunity through coordination with staff counterparts and other commands.

a. Advantages. Briefings are an effective way to disseminate intelligence quickly. They permit interaction with the intended audience, and the audience can provide instant feedback to the briefer concerning content, conclusions, and questions or new IRs. In non-tactical situations--and given sufficient lead-time--formal briefings can be supplemented with multimedia products that create long-lasting visual memories. In combat situations, intelligence can be relayed rapidly through short oral updates that explain or estimate changes regarding the threat, environment or friendly intelligence operations.

b. Disadvantages. Preparation for briefings can be time-consuming in an already time-constrained situation. To convey a large amount of intelligence, hardcopy hand-outs or graphics covering key briefing points should accompany the oral presentation. Time constraints, however, may preclude this. Further, briefings usually reach only a selected audience in a tactical situation--such as the commander's staff. To compensate for this, G/S-2 personnel are encouraged to videotape key briefings or prepare concise intelligence reports in order to disseminate critical intelligence to subordinate units and other external organizations.

7003. Common Forms of Briefings. *Common forms of briefings include the information brief, decision brief, and confirmation brief.*

a. Information Brief. The most common form of briefing given by the intelligence Marine is the information brief. Its primary purposes are initial situation orientation for initial planning and to enhance situational awareness and understanding. Common examples are the initial staff orientation enemy, weather and terrain brief and the commander's morning update or "boardwalk" brief.

b. Decision Brief. A second common form is the decision brief, with the intended purpose of getting a decision from the commander. An example would be briefings conducted to convey the

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

results of wargaming and gain a decision from the commander regarding his desired course of action, allocation of forces and resources, and priorities.

c. Confirmation Brief. A third type of briefing is a confirmation brief, which is conducted as a final review of a planned action to ensure those participating are certain of the objectives and synchronized with each other.

7004. Intelligence Information Brief Format

a. Overview. Of the three most common types of military briefings --information, decision, and confirmation-- intelligence personnel will most often be required to provide intelligence information briefings. The intent of the intelligence information brief is to enhance situational awareness and impart understanding. Intelligence information briefings may be as simple as a quick verbal update to a commander in front of a situation map, or as complex as a MEF or JTF level daily update to the commanding general and his staff. Briefings at lower tactical levels, where the element of time is often scarce, will be generally less formal, but often short-notice. Higher commands generally employ regular, scheduled, daily update briefings, of which intelligence is only one part. Regardless of the degree of formality or the level of command, a standard briefing format or outline can assist intelligence personnel in rapidly and effectively organizing for the brief.

b. Guidance. The keys to developing and delivering an effective intelligence information brief are as follows:

- **Know your audience.** Is it the commander, his staff, his subordinate commanders? Who is the focus of the brief? What is their level of knowledge concerning the subject? Does the commander have any personal preferences as to how he is briefed?
- **Be sure of the purpose and intent of the briefing.** Is the brief an update on critical events in the last couple of hours, or is it intended to describe in detail the threat and area of operations prior to the initiation of crisis action planning?
- **Concentrate on essential information and intelligence,** but be prepared to provide details or expanded intelligence should questions arise.
- **Use clear, concise, readable graphics.** If presenting to a large audience, ensure the graphics can be seen from the rear of the room or, at a minimum, by your primary target audience.
- **Know your information.** If you anticipate questions on subjects where you have little depth, either arrange to have someone there that does, or take the question for follow-up research. Admit when you don't know something; never make up an answer.
- **Always distinguish between what you know (facts), what you don't know (gaps), and what you think (estimates).**

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

c. “Boardwalk” Brief. The most common types of intelligence information briefing are the “boardwalk” and, at higher command echelons, the commander’s morning/evening update briefs. The boardwalk is an informal, on-demand brief conducted using the COC map boards or screen displays from automated systems. The brief is generally by exception, meaning only significant changes to threat capabilities or courses of action are briefed. It is also an opportunity for the commander to ask directed questions.

d. Commander’s Update Brief. The morning/evening update briefs are usually more formal and detailed. As the name implies, they are scheduled for set times either once or twice per day, the schedule being determined by the planning, decision execution, and assessment (PDE&A) cycle or unit SOP. In addition to briefing the current situation and significant events, the brief may also address the commander’s PIRs, collection/production/dissemination plans and status, weather, and estimates of future threat actions. Intelligence may be only part of the overall briefing, and often the briefing is presented using software such as Microsoft PowerPoint.

e. PIR Focus. The principal general guide for what to brief in either case is by orienting on the commander’s PIRs. By focusing on intelligence and events that correspond to the commander’s PIRs, the briefer not only has a quick method of organizing the information and intelligence, but also ensures that the commander is given the most essential information in the shortest amount of time. This does not preclude additional information being presented; if something of significance occurs that will affect the current or future plans, the commander must be informed. Good judgment must prevail.

f. Content. Below are listed the elements of an example update briefing. Note that the elements closely follow the elements of the web-based graphic INTSUM. Given that both are often created in software such as PowerPoint – and in essence provide the same intelligence and other information – using the same format and graphics can save time and resources.

- Weather
- Weather Effects Assessment
- PIRs and IRs
- Situation (ground, air, air defense, etc., all keyed to PIRs)
- Collection, production, and dissemination plans/status
- Intelligence estimate (at a minimum, most likely and most dangerous enemy courses of action)

Note: To save time, those categories that have not changed since the last briefing can be briefed as “no change.” Generally, however, the weather forecast, PIRs, plans status, and intelligence estimate should always be briefed.

7005. Types of Briefings. Appendix D provides sample formats for common types of MAGTF intelligence briefings.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

a. Initial Intelligence Orientation Brief

(1) Purpose. The purpose of the initial intelligence orientation brief is to disseminate important characteristics of the AO and the threat. Its goal is to indoctrinate key personnel to the overall intelligence perspective concerning an impending operation and to help rapidly focus commanders and key planners on mission critical factors.

(2) Content. The initial intelligence orientation brief should generally follow the intelligence estimate format, supplying all relevant intelligence on the AO and the enemy. Much of the content of this type briefing is derived from higher-echelon studies and estimates and is presented as background basic intelligence. Because this type briefing can easily become too long or too overwhelming in detail for timely dissemination, particular care should be exercised to employ graphics wherever possible.

b. Intelligence Estimate of Supportability

(1) Purpose. The purpose of an intelligence estimate of supportability briefing is to evaluate friendly COAs based on the capabilities and limitations of organic and supporting intelligence, CI, and reconnaissance forces. Its goal is to assist the commander in understanding intelligence operations capabilities, alongside all other friendly functional capabilities, in order to decide the most promising friendly COA and to identify IRs.

(2) Content. The intelligence estimate of supportability brief addresses key factors identified by intelligence personnel that may influence friendly intelligence operations. These key factors include terrain; weather; the current political situation; possible reactions from the civilian populace; the enemy's relative strengths, weaknesses, and susceptibility to friendly deception or psychological operations. The briefing then addresses enemy COAs, analyzes enemy COAs versus friendly COAs based on the key factors, identifies the preferred friendly COA, and offers any other recommendations to the commander.

(3) Approaches. The particular approach used by the briefer will vary based upon commanders' preference, nature of the operation, complexity and scope of friendly intelligence operations, echelon of command, or other METT-T factors. Two useful approaches are:

- **Threat COA Focused.** The intelligence estimate of supportability brief will address each current estimated threat COA, associated PIRs and other key IRs, probable friendly collection and production operations, and significant gaps or deficiencies.
- **Friendly COA Focused.** With this approach, the briefer will detail probable collection and production operations and significant gaps or deficiencies for each friendly COA under consideration.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

c. Mission/Target Intelligence Brief

(1) Purpose. The purpose of the mission/target intelligence brief is to provide detailed and tailored intelligence to support execution of a specific mission. Examples of such missions include reconnaissance unit inserts and operations, raids, and noncombatant evacuation operations (NEOs). The goal is to provide timely and relevant intelligence to support mission accomplishment.

(2) Content. The mission/target intelligence brief has no prescribed format but should contain all pertinent intelligence impacting on a specific mission or target. A superb starting point for organizing and preparing such briefs is the “*Mission Profiles*” section of the *Generic Intelligence Requirements Handbook* published by the Marine Corps Intelligence Activity. Examples include a ground reconnaissance unit mission brief, aircrew mission brief, and raid site brief. Normally, this type briefing provides any intelligence and other information on activity occurring or expected to occur within a predetermined radius from the target/mission and within a predetermined amount of time from target/mission commencement. At a minimum, it should include an area orientation and detailed descriptions of entry points, the objective area, and threat composition, locations, dispositions, capabilities and vulnerabilities. Graphics should be employed extensively to quickly portray potential enemy COAs strengths and vulnerabilities in response to friendly operations.

d. Intelligence Update

(1) Purpose. The purpose of the intelligence update brief is to review intelligence activity since the last briefing, to present the current intelligence situation, and to estimate anticipated enemy activities that may affect friendly COAs. Intelligence updates are usually scheduled briefings and are designed to address predetermined periods of time such as every 12 or 24 hours. Examples include watch turnover briefs in the unit COC, IOC, or SARC.

(2) Content. The intelligence update brief follows a temporal outline, commencing with the reporting of any significant enemy activity--including any enemy losses--since the last update. It then presents the current enemy situation, followed by weather forecasts and intelligence estimates of enemy COAs and activity during the next reporting period. The update should also address any current or impending friendly intelligence collection, production and dissemination operations that could supplement intelligence disseminated in the briefing.

e. Technical Intelligence Brief

(1) Purpose. The purpose of the technical intelligence brief is to provide detailed intelligence on a specific enemy weapon system, piece of equipment, or functional capability and limitations. This type of briefing is used to disseminate a substantial amount of technical and scientific intelligence in a condensed format.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(2) Content. The technical intelligence brief has no prescribed form but should, at a minimum, provide a detailed description of the threat or weapon system and its attendant characteristics, capabilities, and vulnerabilities. If the system has associated unique visual or electronic signatures, ensure all known operating parameters are disseminated to intelligence, targeting and key maneuver personnel. The briefing should also describe how the enemy employs the system (i.e., tactics, processes and procedures) and where it is currently deployed (i.e., OOB). Graphics should be used wherever possible to quickly convey this type of complex information.

7006. Preparation Principles. *The #1 requirement for any intelligence briefing is that it focuses on the commander's PIRs and key planner IRs. The three chief principles of briefings are accuracy, brevity, and clarity. Dissemination considerations must take all three into account.*

a. Accuracy. In achieving accuracy, ensure that source reliability--often found in reference material--is conveyed to the audience. Unless specifically asked, do not offer personal opinions. (Note: Refer to Chapter 3, "Analytical Thinking," of MCWP 2-12, *MAGTF Intelligence Analysis and Production* for a detailed review of intelligence analytical methodologies, the forms of reasoning, and analytical pitfalls.)

b. Brevity. In striving for brevity, resist the temptation to disseminate all that is known on a topic. The commander's guidance and PIRs, current and estimated situation, and planned friendly actions will help focus briefs on what is important and what is not. In planning how to use the time available for the brief, always incorporate sufficient time for questions from the audience.

c. Clarity. In attaining clarity, present the intelligence and other information as clearly as possible--both orally and graphically. Use short and crisp sentences. Define any unfamiliar terms or acronyms, ensure any item referred to orally is depicted in the corresponding graphic, and summarize key points at the end of the presentation. Most importantly of all, keep the brief focused on the PIRs and other IRs that it is providing intelligence in response to.

7007. Intelligence Briefing Methodology. The same methodology applies to both formal and time-sensitive tactical intelligence briefings, differing only in time available and level and detail of the IRs and intelligence to be provided.

- **Formal intelligence briefings** usually are allocated more lead-time and require a more structured methodology in disseminating information. Generally, such briefings will address a broader range of IRs and other intelligence needs. Also, such briefings typically entail a more open-ended timeframe. The intelligence estimate format usually provides the departure point for these briefings.
- **Time-sensitive tactical intelligence briefings** should follow the format of formal briefings as much as time allows. Given that lead-times for briefings are much shorter in a field environment however, tactical briefing formats vary widely. Ones most frequently used include:

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

1. Standard TACREP or SALUTE format
2. Standard INTREP format (see appendix F)
3. Use if DRAW-D framework. At a minimum, the most likely and most dangerous threat options should always be briefed.

Figure 7-1 depicts six steps for preparing an intelligence briefing. A more extensive guide for preparing formal intelligence briefings is provided in Appendix E.

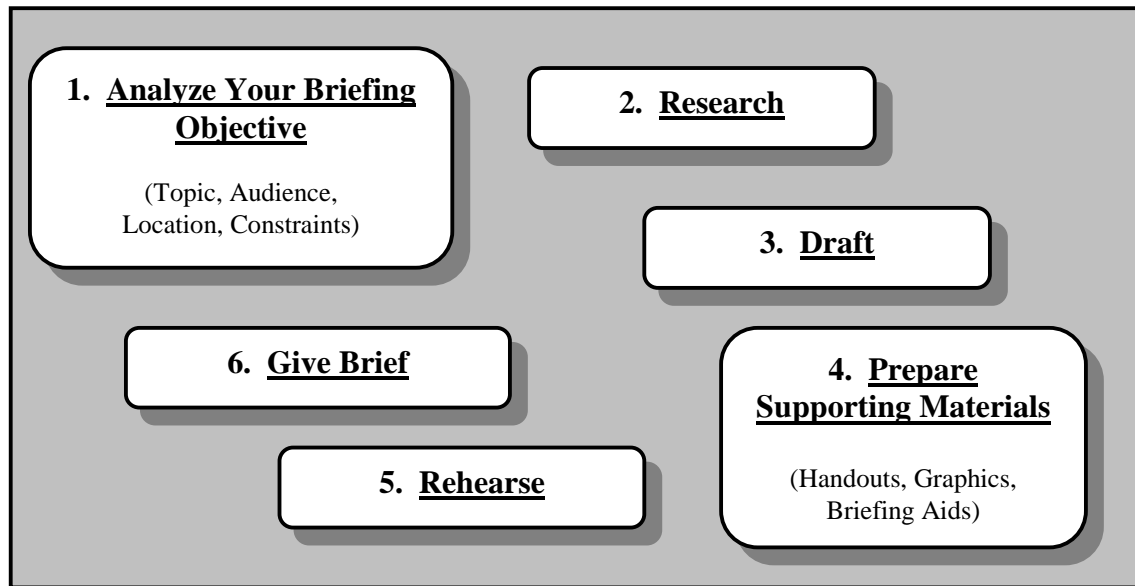


Figure 7-1. Briefing Preparation Steps

a. Analyze Your Briefing Objectives – The “Five W’s and H: Who, What, Where, When, Why and How -- to aid with briefing preparations.

- **Who?** Audience's background – commanders, planners and others? Familiarity with topic? How much technical detail? Also, which intelligence personnel will give the brief? And which others are needed for questions and other support?
- **What?** Related PIRs and IRs? If topic is assigned, what is required? If topic is chosen, what is the scope? What must the audience take away to understand the briefing and immediately use the provided intelligence?
- **When?** What day and time is the briefing? How much time is allotted for the briefing? What intelligence cut-off time will be used?
- **Where?** What facilities are available? Any distractions at briefing site such as a nearby runway (noise) or commercial facilities (security)?

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

- **Why?** What is the purpose of the briefing? How does it relate to the audience? How can the audience best use the information disseminated in the briefing? Would the audience benefit from hand-outs to take away from the briefing? How does this briefing fit into the overall briefing schedule?
- **How?** What audiovisual or information technology equipment will be available and how does it work? What other equipment must be brought? Will the audience all be physically present, or will some be via VTC or other means? Who will record questions or new IRs that will require follow-up action? What other intelligence products are/will be developed that may reinforce the brief?

b. Research. The PIRs/IRs will drive your research efforts! Access all available intelligence reference material to learn as much as possible concerning the briefing topic. Allow lead-time to request information and intelligence not easily accessed at local commands. As research progresses, ensure notecards are prepared to consult later in answering questions. Reduce quantity of intelligence in favor of increasing quality of briefing. Use the intelligence cut-off date/time previously selected.

c. Draft. Organize information, intelligence and other materials in a logical fashion--functionally, geographically, temporally, threat/friendly COAs, etc. Make an outline from these and later fill in key words, phrases, quotations, facts, and graphics. Ensure the outline follows an "introduction, body, conclusion" format and carries appropriate security classifications.

d. Prepare Supporting Materials. Decide how to disseminate the intelligence. Prepare maps and charts in colorful and readable formats and ensure there are no misspellings. Decide in advance if pointers, lecterns, or special lighting are needed. Coordinate closely with other intelligence personnel preparing reinforcing intelligence products.

e. Rehearse. Enlist a willing audience from staff colleagues to practice presentation delivery. Rehearse as many times as necessary to gain confidence and proper tempo of the briefing. Time all rehearsals, using all planned graphics or special effects. Key: Do a last check with intelligence analysts and check principal intelligence references to confirm the currency and accuracy of your brief!

f. Give Brief. Arrive early enough to ensure the location and all equipment are prepared and operational. Also, use available time to determine if the audience will include any significant changes or if any unanticipated questions are likely. Then, give the brief. Remain focused on the IRs and other objectives. Answer all questions to the best of your ability. Also, ensure someone else records all unanswered questions or new IRs: who asked, unit/section, telephone numbers, special needs, and if any response times were promised.

Chapter 8

Intelligence Reports

8001. Overview. This chapter focuses on common discipline-specific and all-source intelligence reports. Appendix F provides basic formats for the all-source intelligence reports discussed in this chapter. Intelligence discipline-unique reports are addressed in other intelligence series MCWPs and MCRPs.

a. Purpose of Intelligence Reports. *The purpose of generating intelligence reports is to disseminate intelligence quickly to a wide audience for immediate use.* If generated and disseminated judiciously, reports provide excellent support for each of the six intelligence functions: support to the commander's estimate, situation development, I&W, support to force protection, support to targeting, and support to combat assessment. Because reports normally contain perishable intelligence, they usually are transmitted by secure radio, digital datalink, e-mail, telephone, facsimile or message. Intelligence reports should be disseminated in accordance with either collection or reporting criteria or the dissemination plan. *Reports are not a substitute for regular communication between intelligence officers and staff counterparts.* Regular collaboration among all intelligence officers is critical for effective planning and direction, C2, and understanding the use of intelligence.

b. Summary Intelligence Reports. The purpose of summary intelligence reports is to provide the commander with an overview of significant enemy activity within a specified period of time and to project anticipated enemy actions during the next reporting period. *Summary reports are usually scheduled products disseminated at specific times as dictated by unit SOPs or OPLANS/OPORDs.* Standard summary reports, disseminated at scheduled times, are well-suited for demand-pull dissemination, such as being posted on the MAGTF S-TDN. Keep in mind, however, that dissemination below the MSC level may require other means. For example, hard copy dissemination via courier is still often used from MSC to subordinate units (the S-TDN extends to lower echelons), with select dissemination of critical excerpts via other means, such as secure radio or telephone.

c. Specialized Intelligence Reports. Specialized reports include event-driven intelligence reports, such as SALUTE reports, and various intelligence discipline-unique intelligence reports, such as tactical electronic intelligence (TACELINT) reports, initial photographic interpretation reports (IPIRs), CI spot reports, surf observation reports, bridge reports, etc. Specialized reports are disseminated as required. See each of the MCWPs in the MCWP 2-15, *Intelligence Support Series*, for a complete discussion of these reports.

8002. Periodic Summary Text/Voice Intelligence Reports

a. Intelligence Summary (INTSUM). The INTSUM is a text or text/graphic intelligence report that provides a summary of the intelligence situation covering a specific period normally

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

prescribed by the unit SOP for intelligence or the intelligence annex to the operation order (for a MEF-level operation, usually every 12 or 24 hours). It is used to report threat activities, changes to threat capabilities, and the results of further analysis and production. It is designed to update the original and subsequent intelligence estimates. At lower commands, particularly JTFs and combatant commands, a DISUM (or daily intelligence summary) will usually be published every 24 hours. INTSUM distribution will be in accordance with the dissemination plan, but generally will be disseminated at least to immediate higher and subordinate commands. Using the basic format, units can tailor the INTSUM to fit the situation. With new automated information systems, INTSUMs are increasingly produced in graphic form and posted on networks for wide dissemination, with links to detailed supporting intelligence products, reports and databases. The graphic INTSUM is maintained either on computer screens linked to intelligence databases or on conventional maps with displayed/accessible supporting information. See Appendix F for the basic MEF-level INTSUM format. INTSUMs address the following:

INTSUM Topics

Together, the text and graphic INTSUM depicts and reports all current and estimated intelligence concerning enemy:

- Ground, Air, and Naval Activity and Losses
- Movement
- Equipment
- New Units
- Personalities
- Obstacles
- Administrative Data
- Weather and Terrain Conditions
- Capabilities and Vulnerabilities
- Anticipated Enemy Direction.

The INTSUM should also include:

- Unit's Current Threat Estimate – COAs, vulnerabilities
- Revalidation of Previously Stated PIRs
- Identification of New PIRs
- Current and Planned Organic Intelligence Operations.

b. Daily Intelligence Summary (DISUM). At higher command levels, particularly JTFs and Unified Commands, a daily intelligence summary (DISUM) will usually be published every 24 hours. While INTSUMs, particularly at lower tactical echelons, provide a generally fine-grained tactical perspective, the DISUM is broader in scope, potentially encompasses more aspects of a threat country's elements of national power, and focuses on operational-level intelligence analysis and estimates. MAGTF command elements tasked as JTF headquarters will generally be required to submit DISUMs to the combatant command CINC. See the combatant

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

command's TTP for the DISUM format. Although generally the same, formats may vary from theater to theater. DISUMs usually address the following:

DISUM Topics

Prepared in narrative format, the DISUM should address:

- General Enemy Situation
- Enemy Operations During the Reporting Period
- Counterintelligence Situation
- Other Significant Intelligence Events (e.g., OOB changes; new weaponry sightings)

The DISUM should also include:

- Unit's Current Threat Estimate
- Revalidation of Previously Stated PIRs
- Identification of New PIRs
- Current and Planned Organic Intelligence Operations.

Additional information that may be included: BDA intelligence and weather forecasts.

c. Periodic Intelligence Summary (PERINTSUM). The PERINTSUM is an expanded INTSUM covering a greater period of time as dictated by the commander. It is a means for disseminating more detailed intelligence than that provided in INTSUMs or DISUMs. PERINTSUMs are normally issued by the MAGTF CE for higher, lower, and adjacent dissemination. Subordinate units, however, may also be tasked to prepare them if the commander so directs. PERINTSUMs can be either hardcopy or softcopy summaries--complete with available graphics--and should convey all known intelligence collected on the enemy. The format for PERINTSUMs generally is the same as used for DISUMs.

8003. Graphic Intelligence Reports

Graphics should be incorporated into intelligence reports when appropriate, depending on a unit's capability to receive graphic material. Because symbolic representations are especially effective in small unit tactical environments, these units' intelligence and communication officers should attempt to ensure that secure facsimile and digital datalink capabilities are incorporated into intelligence architecture plans.

Sitmaps--with annotations and enhancements such as tables, marginal data, and schematics--are the preferred means of quickly conveying large amounts of current intelligence. Overlays can then provide updates as needed. Supplementary diagrams, imagery, and text should be supplied as required.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

With the exploding use of information technologies, greater standardization of military symbology is essential to enhance interoperability and understanding while minimizing errors. MIL STD 2525B is now the current symbology. Also, use MCRP 5-12A, *Operational Terms and Graphics*, for additional information on military symbology.

8004. Event-Driven Text/Voice Intelligence Reports

The purpose of generating event-driven intelligence reports is to disseminate significant intelligence to the commander or to intelligence operations personnel that could immediately alter the tactical situation or to support situation development. Event-driven intelligence reports are generated as required. Detailed direction will be established in either current collection reporting criteria or the dissemination plan. To further manage this, dissemination planners – in coordination with collection and production planners -- should establish reporting thresholds.

a. SALUTE Report. The SALUTE report is a basic intelligence report that may be used by any unit to report key intelligence information. Its contents are those of the acronym SALUTE: Size, Activity, Location, Unit, Time of Observation, and Equipment. SALUTE reports may be used for either routine or time-sensitive intelligence reporting. They are issued by any unit--normally MAGTF subordinate entities--observing or in contact with enemy forces or as otherwise directed in the current reporting criteria. They are disseminated at the highest precedence possible, usually via secure voice radio transmission, to a predetermined distribution. If time permits, secondary dissemination should be generated via electronic data transmission. See Appendix F for the SALUTE report format.

b. Intelligence Report (INTREP). The INTREP is a standardized report which, based on its importance to the current situation, is disseminated without regard to a specific time schedule. That is, an INTREP is not prepared on a periodic basis, but as information is acquired, assessed and intelligence estimates are produced. It is the primary means for transmitting new and significant intelligence when facts influencing threat capabilities have been observed, or when a change in threat capabilities has taken place. It is prepared at all echelons by the first intelligence element acquiring the information and forming the intelligence estimate, and is disseminated as rapidly as possible to all units which may have need of the reported information. It may be prepared on any item of intelligence, regardless of source. Generally each report will concern only a single item. When time permits, the INTREP should include the originator's interpretation of the information or intelligence being reported. See Appendix F for the INTREP format.

c. BDA Reporting. The intelligence officer (at the MEF CE level, the ISC) ensures BDA reports conform to the operational plan, report the nature of damage inflicted or unit/systems destroyed, and assess the degree of mission success as it relates to the initial objective. When possible, BDA reporting includes the physical damage assessment and an analysis of the consequence of the damage on the threat unit. The intelligence officer or ISC must attempt to obtain visual verification of the target damage and destruction.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

MAGTFs and their subordinate elements are primarily concerned with conducting Phase I BDA/physical damage assessment (PDA). Sources of information for Phase I/BDA include:

- Mission reports (MISREPs) and in-flight reports (INFLTREPs)
- Aircraft cockpit video (ACV) or weapons systems video (WSV)
- Imagery and IMINT including national, theater, and tactical imaging systems and UAVs
- Signals intelligence (SIGINT)
- Human resource intelligence (HUMINT)
- Open source intelligence (OSINT), including television and radio broadcasts, newspapers, etc.
- Visual reports from combat units, air controllers, or forward observers.

At each echelon, the intelligence officer compiles, refines, and validates the various sources of BDA and develops consolidated PDAs and/or combat strength assessments. The MSCs/MSEs will forward consolidated BDA reporting of their subordinates and forward a summary BDA report to the MEF, usually covering set time periods. See Appendix F for an example of a summary BDA report format.

At the MEF level, the P&A Co, intel battalion, is responsible for compiling the overall Phase I/PDAs for the MEF, and for adjusting the master OOB databases to reflect threat combat losses. The BDA Cell will also prepare and disseminate formal Phase I BDA reports in accordance with theater and national policies and procedures. The DIA Defense Intelligence Reference Document, *Battle Damage Assessment (BDA) Reference Handbook* (U), DI-2820-1-97, provides detailed joint procedures for formats regarding BDA analysis, reporting formats, standard terminology, and resources. This document is available on-line via INTELINK-S and INTELINK. See Chapter 7 of MCWP 2-12 for additional information on BDA analysis and reporting.

d. Mission Report (MISREP). Mission Reports (MISREPs) are used by aviation units to report significant results of aircraft missions and non-imagery sightings along flight routes. They employ a standardized format that includes air task/mission number or nickname, location identifiers, time on target/time of sighting, results/sighting information, and remarks. Upon completion of post-flight debriefing, squadron S-2s should disseminate MISREPs to the MAGTF G/S-2 by the most expeditious means possible. See Appendix F for the MISREP format.

e. Response to a Request for Intelligence (RRFI). RRFIs are non-scheduled products designed to fill gaps in knowledge identified by subordinate tactical units. In short, they are used to provide specific intelligence to the user requesting it. Because IRs are normally tagged with

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

an LTIOV requirement, RRFIs should be answered and disseminated as quickly as possible. If time does not allow for electronic data transmission, then responses should be distributed over secure telephone or radio. Appendix F provides a sample RRFI format; specific formats used will be per unit SOP.

8005. Intelligence Reports Plan and Matrix. METT-T factors will influence the types, uses, formats and dissemination of intelligence reports during a particular operation. While well developed and practiced SOPs are invaluable, for most operations detailed guidance and instructions must be established to ensure MAGTF-wide effectiveness, efficiency and accuracy.

An effective technique to accomplish this and achieve widespread understanding is the use of an *intelligence reports matrix*. The CMDO is responsible for its development and updating. The particular format of the matrix will be per unit SOP; see Appendix J for one useful format. The intelligence reports matrix will be an exhibit to the intelligence reports tab to the intelligence operations plan of an OPLAN/OPORD's Annex B.

8006. Intelligence Report Preparation. The process for preparing intelligence reports for dissemination generally follows the *five W's and H* analytical process used for estimates/studies and briefings. You must determine what intelligence is needed, who needs it, what the deadlines are for utilization, and where recipients are located within the architecture. To enhance effective dissemination of reports:

- **Select formats for internal MAGTF reporting.** For internal MAGTF use, dissemination can be done via LAN, voice, facsimile, and courier. Standardized intelligence reports are to be used by all MAGTF units, with modifications in accordance with unit SOP only when absolutely necessary. If modified, format changes should be kept to a minimum to preclude disrupting MAGTF interoperability (e.g., standardization is especially critical to allow immediate and smooth interoperability with Marine forces globally sourced from outside the parent MEF). Indeed, to enhance intelligence flow, templates for report formats should already be built into word processing and other software. Free-text reporting formats are acceptable if timeliness is critical.
- **Select formats for external reporting.** For dissemination of MAGTF intelligence reports external to the MAGTF, reporting must adhere to the formats and guidance from the JTF or the combatant command's TTP.
- **Preformat and preprogram.** Construct preformatted templates and preprogrammed distribution lists (IP addresses, etc.) prior to operations. For globally sourced Marine units and all non-Marine forces, close cooperation among intelligence officers is critical to ensure full accuracy, understanding and capability.
- **Reduce voice report contents to the bare minimum.** Keep it simple and short to preclude possible misunderstandings and facilitate timeliness. This objective is significantly enhanced through the use of standardized reports formats and regular training – both of those initiating

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 such reports as well as all intelligence, operations, fires and other Marines who may receive
2 such reports.

- 3
- 4 • **Cross-check data elements.** All data elements contained in intelligence reports should be
5 cross-checked for accuracy before dissemination, particularly numerical elements such as
6 geographical or grid coordinates, times, and enemy unit designations.
 - 7
 - 8 • **Avoid circular reporting.** Reports should convey new information and intelligence. In the
9 event other intelligence must be included in the report for understanding, care must be taken
10 to ensure such intelligence is clearly identified to preclude confusion, false confirmations, or
11 other errors.
 - 12
 - 13
 - 14
 - 15

Chapter 9

**Intelligence Dissemination and Support to the
MAGTF's Common Tactical Picture**

9001. General. The common operational picture (COP) and common tactical picture (CTP) is the means by which all MAGTF commanders develop the situation – i.e., see the operation. When maintained properly, the CTP will provide all a near real-time view of both friendly and enemy forces – and thus tremendously improved command and control, planning, and decision making capabilities than have ever been possible in the past.

Joint and all services doctrine and TTP on COP and CTP concepts of operations and management, however, remain in their infancy. The most useful broad guidance today on this are contained in the following:

- CJCSI 3151.01, *Global Command and Control System Common Operational Picture Reporting Requirements* (10 June 1997)
- MCRP 6-23A, *Joint Task Force Information Management*¹
- MCWP 6-2, *MAGTF Command and Control* (draft, January 2000)
- MCWP 6-23, *Information Management* (draft anticipated Spring 2000)

The pace of information technology development along with many innovative operational and warfighting functional developments, however, clearly indicate significant changes in COP and CTP operations as new procedural and technical capabilities advance.

Because of this, Marine Corps intelligence doctrine and TTP is likewise in its infancy. The following information is provided as an initial foundation to support Service requirements. It is drawn from the best intelligence SOP now in use within the operating forces. For exercise or actual operation support, close coordination between intelligence planners and the G/S-3 information management officer, the G/S-6, and all subordinate units' intelligence officers is critical to ensure full understanding of the process and procedures that will be used to establish and maintain the COP/CTP during the operation.

9002. MAGTF CTP Concept of Operations. Each echelon of command, beginning at the tactical maneuver battalion/aviation squadron level, reports and manages the track database for its own units and those attached to or in direct support of it. Track data will be auto-forwarded via broadcast up to the next higher echelon until it reaches the MAGTF CE. Once

¹ This publication is a multiservice tactics, techniques and procedures publication that all four services have concurred with.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

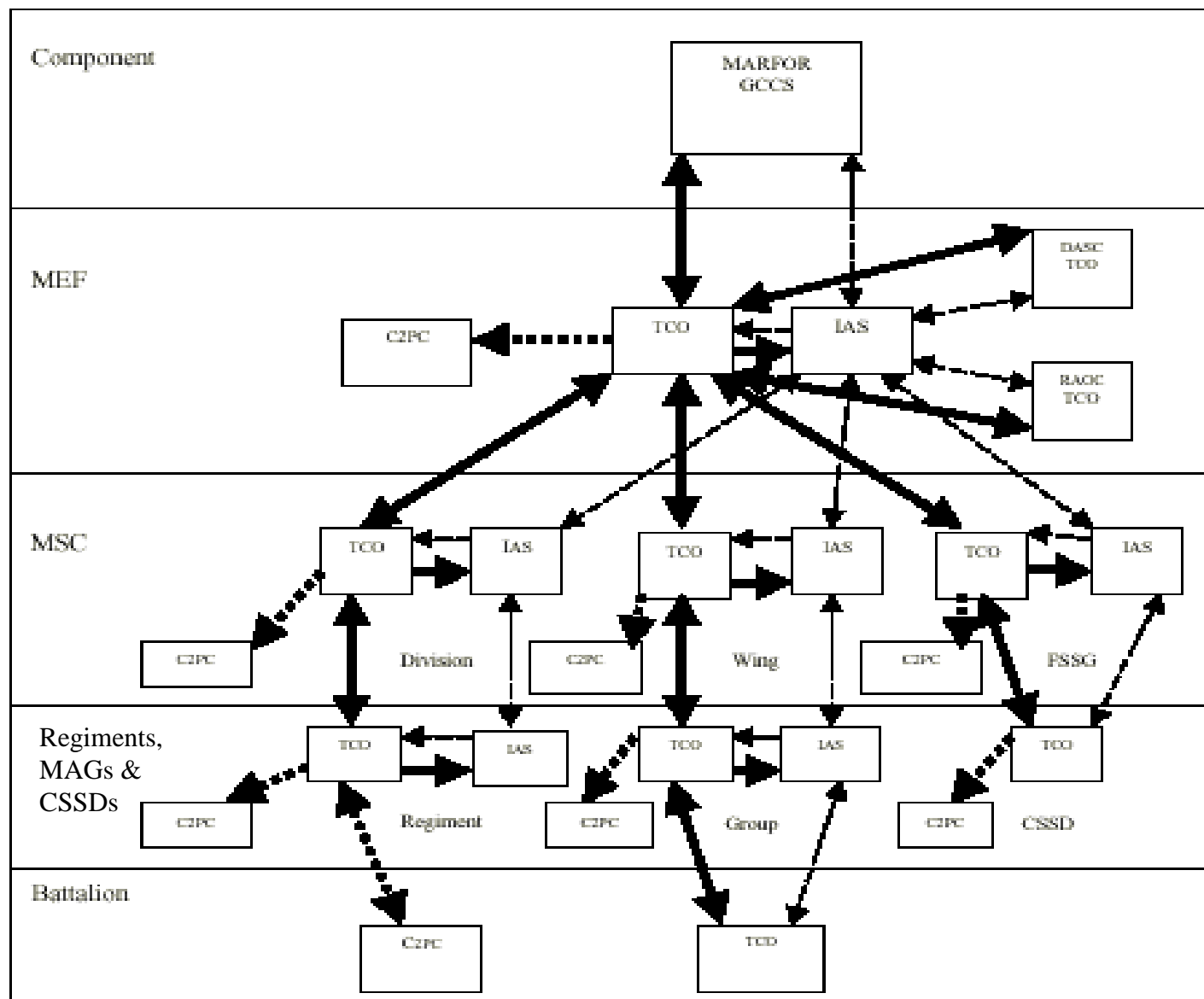
correlated, track data is rebroadcasted back down to each subsequent echelon as the MAGTF CTP. As track data is updated it automatically updates each echelon database and CTP. Auto-forwarding and broadcast times for each echelon must be set correctly or “track looping” may occur. Track looping is an anomaly within a networked system where creation, editing or delete commands pass one another in transmission without accomplishing the desired effect. For example, if the division and its regiments are broadcasting at the same time interval, the regimental TCO delete command would transmit at the same time the division TCO CTP broadcast is being transmitted. Thus, a track a regiment is trying to delete remains in the system causing a “track loop”. Additionally, if broadcasts are too frequent it will slow down the entire TDN.

9003. MAGTF CTP Planning. Prior to employing the system during a deployment or contingency, key planners will meet to coordinate CTP efforts. These meetings will be directed by the G/S-3 information management officer and include all staff system administrators, G/S-6 representatives, and G/S-2 and G/S-3 representatives. Key tasks will be to coordinate IP addresses, broadcast parameters and physical layout. Senior/subordinate relations will also be refined, and additional directives from the higher commands will be declared. Additionally, any component issues will be raised, clarified and resolved.

9004. Architecture. Figure 9-1 depicts a typical notional operational network architecture for CTP actions. Figure 9-2 provides a more granular depiction of the architecture within the MAGTF CE’s main command echelon. Regiments, MAGs and CSSDs will normally be the first points where friendly and threat unit locations are inputted. These echelons will electronically plot their battalions, companies, etc. A command will only update information for those units assigned under its command, or those attached or in direct support to it. These echelons will auto-forward all track data, via broadcast or via the S-TDN, to the next higher echelon. This information will enter the MSC headquarters system as “ambiguities” that need to be resolved before further broadcast. The MSCs’ information management officers (IMOs) coordinate resolution of these ambiguities, ensuring that the track data is correct, input any additional required track data, and broadcast that track data up to the MAGTF CE. The MAGTF CE receives ambiguities as well. Resolution of these likewise will be coordinated by the MAGTF IMO, with results then inputted into the track database. These tracks as well as the tracks the MAGTF CE is required to input into the broader JTF CTP/COP will then be auto-forwarded up to the MARFOR or JTF, and rebroadcast down the chain to all MSCs. In turn, the MSCs will rebroadcast these tracks down to the regiments, MAGs and CSSDs.

This comprises the CTP. A track creates an ambiguity only when first entered into a system. From that point on the track will automatically update as its owner makes changes. **Only the creator/owner will edit or delete a track in their database in accordance with the overall MAGTF CE assignment of responsibilities (see annex U to the OPLAN or OPORD).** Additionally, broadcast and display filters will be used to define what type of tracks will be transmitted and/or displayed.

1
2
3



39
40
41
42
43
44
45

Figure 9-1. MAGTF CTP Notional Network Architecture

1
2
3
4
5
~

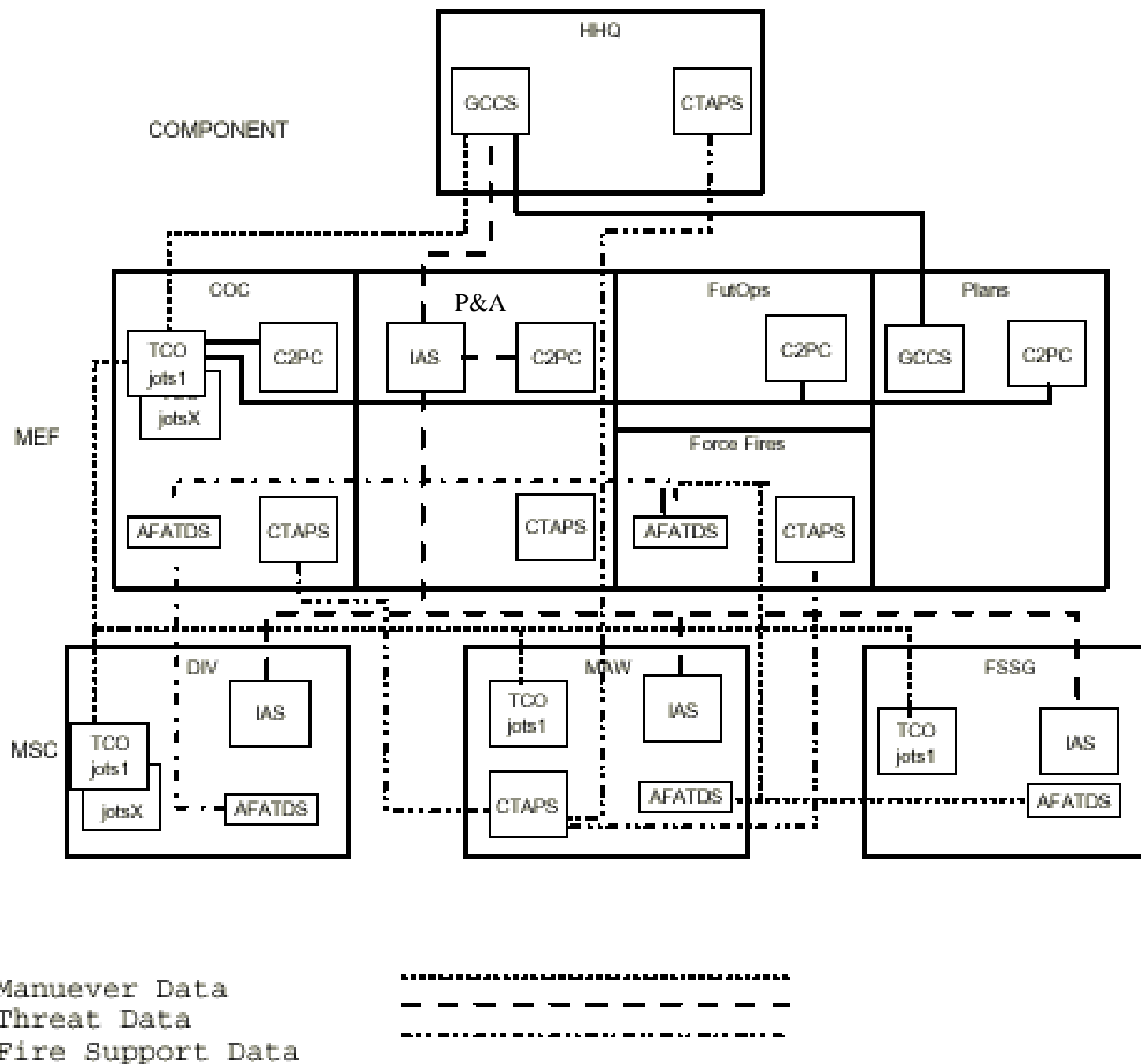


Figure 9-2. MAGTF CE Main Command Echelon Notional Network Architecture

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

9005. Responsibilities.

a. MAGTF Command Element. The MAGTF CE is the hub for CTP data receipts and transmissions. All information received at this level is auto-forwarded down via broadcast to all MAGTF MSCs, and externally to the the MARFOR or JTF headquarters as the MAGTF's CTP (in accordance with the JTF's COP/CTP reporting criteria established in the JTF's information management plan). All new tracks must be validated prior to forwarding; the IMO will coordinate this effort overall for the MAGTF CE. Additionally, the G/S-3 COC watch officer and the P&A Cell OIC must closely coordinate to provide each other with friendly and threat track data respectively. The following is germane.

(1) BLUE FORCE Track Management -- G/S-3 COC Watch Officer Responsibility. The COC uses the TCO system for tracking friendly unit positions. The G/S-3's COC Track Manager is responsible for managing ground Blue Force (friendly) track data received from the MAGTF's subordinate commands. The COC Track Manager will de-conflict and consolidate Blue Force data and then broadcast the CTP to the network, to include G-2 COC and FOC watch officers and all key nodes within intel bn's IOC. The G/S-3 COC watch officer is further responsible for updating friendly unit locations as prescribed by the MAGTF's information management plan.

(2) RED FORCE Track Management

(a) P&A Cell OIC Responsibility. The P&A Cell uses the IAS system to conduct analysis of enemy track data. The P&A Cell's track manager is responsible for managing threat data received from the MAGTF's subordinate commands. Once the P&A Cell is aware of a threat unit's location, the P&A Cell Track Manager will generate a new threat track, annotate required analyst comments, and forward that track to the G/S-3's COC Track Manager. The P&A Cell OIC is further responsible for updating threat unit locations as prescribed by the MAGTF's information management plan.

(b) CMDO Responsibility. The CMDO, through the intelligence systems officers, is responsible for intelligence systems and technical support to maintenance of the Red Force track management within the CTP.

(3) Friendly Intelligence, CI and Reconnaissance Units Track Management. The ISC is responsible for accurate maintenance of friendly intelligence, CI and reconnaissance units tracks within the Blue Force CTP.

b. MSC Responsibility. MEF MSCs also transmit via auto-forward friendly and threat broadcasts both up and down the chain. They receive their initial data information from the regiments, MAGs and CSSDs, and auto-forward it to the MAGTF CE. Likewise, they receive data information from the MAGTF CE and auto-forward it back down to the regiments, MAGs and CSSDs. Thus, each echelon has the same CTP and track database. Each MSCs COC G/S-3 watch officer and G/S-2 intelligence operations officer is responsible respectively for their echelon's blue and red track data and coordinating their interaction within the command echelon.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

c. Regiment/MAG/CSSD Responsibility. Regiments, MAGs and CSSDs have the TCO and IAS systems to support their CTP requirements. They will also send and receive track data to and from the next higher echelon. These units will also share friendly and enemy track data in the same fashion as the MAGTF CE and MSC headquarters.

d. Other Units Responsibility. Other units that require a CTP from the MAGTF CE or a MSC headquarters will coordinate directly with that unit's G/S-3 COC watch officer and ISC/intelligence operations officers. The same basic requirements apply: they are to provide track data for themselves. They generally do not provide any enemy track data. However, should the need arise to pass such enemy track data, the P&A Cell OIC or intelligence operations officer should be included in any decision to pass such traffic. Non-USMC units normally do not have systems that allow them to input into the CTP. Instead, their data must be inputted manually at the lowest possible level.

e. Reporting. The IMO at each echelon of command is overall responsible for de-conflicting data received from lower echelons, working in close coordination with the COC G/S-3 and P&A Cell OIC. Blue force track data will be forwarded to the MAGTF COC via a "filtered" S-TDN broadcast allowing only Blue Force track data to be sent. A "continual threat data assessment" will be conducted by the P&A Cell OIC on Red Force track data received from organic assets. Upon completion of the "immediate assessment," the threat data will be forwarded via a "filtered" S-TDN broadcast to allow only threat track data to be sent.

9006. MEF G-2/IOC CTP Operations

a. Background. There are several crucial steps in the process of creating and maintaining an accurate Red Force picture within the MEF CTP.

(1) First, it is essential that the unit locations are created and entered correctly into the IAS.

(2) Second, MEF MSCs are given ownership of threat units which are resident in their AORs. Positive control of every threat track is essential in maintaining an accurate CTP. The MSC's AOR will be determined by the MEF by the use of geographical boundaries, which assign ownership of threat tracks to the MSCs.

(3) Third, only the MSCs responsible for a given threat track may edit, move, or delete that track. The CTP is in jeopardy of corruption when a threat track crosses a geographical boundary, and either no one or multiple MSCs are editing that threat track. Thus, the need to maintain positive control.

Friendly tracks are transmitted to the MEF IAS via broadcast from the G-3. This broadcast occurs at a regular time intervals according to G-3 information management SOP. The friendly CTP is also broadcast to each of the MSCs from G-3 TCO to MSC's TCO according to the G-3 information management SOP. *Only threat tracks will be broadcast from the MEF IAS to the MSCs' IAS'.*

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

b. Procedures

(1) MEF CE G-2/Intelligence Battalion. The MEF G-2 is responsible for the overall Red Force track management within the CTP. He executes this responsibility through the ISC. Through the use of a **Track Management Matrix** and battlespace boundaries, the MEF AC/S G-2 will assign ownership of threat tracks to the MSCs. The Track Management Matrix defines the MSC's AOR and identifies the number and location of the threat tracks that belong to each MSC. This generally is merely a textual version of the geographical boundaries set by the MEF G-3. In general, the GCE is responsible for the threat ground order of battle (GOB) in their zone. The ACE is responsible for the air order of battle (AOB) minus surface to surface missiles. The CSSE or Rear Area Operation Group (RAOG) has responsibility of the rear area, if not already assigned to the IOC. Finally, the IOC is responsible for the deep battle (portions of the AOR's CTP not being covered by the MSCs). Geographical boundaries depict the MSC's battlespace as their area of responsibility for the CTP. This information is then manually entered into the IAS. Once all the threat tracks have been entered into the IAS, a broadcast is sent to each of the MSC's IAS, as well as to the MEF TOC within the COC and FOC.

(2) MSCs

(a) The MSCs have control of all the threat tracks within their AOR. As these tracks move or change, the MSC will send manual transmissions, via IAS, to the MEF IAS. Additionally, the MSC must communicate the change using one of the following methods: IAS-to-IAS chat, secure phone, or e-mail (in order of priority). These are also the recommended means of coordination and troubleshooting. Once an hour, each of the MSCs will count the exact number of tracks in their AOR and then transmit that number to the MEF P&A Cell via one of the above means. This will ensure every track is being maintained. MSCs may transmit and receive track data with their subordinates via means consistent with their unit SOPs.

(b) It is essential that the MSCs validate tracks transmitted to the MEF. Once received in the P&A Cell's IAS, tracks are broadcast to all MEF subordinates and to the MEF COC, FOC and other nodes via auto-forward. Therefore, tracks sent in error can quickly propagate throughout the entire CTP. As a backstop, MSCs are requested to backup their CTP to 8mm tape at least every two hours to enable data recovery in the event of system failure or accidental deletion. Also, the P&A Cell OIC will provide the MSCs the entire Red Force CTP via the S-TDN if required.

c. Personnel

(1) Red Force Track Managers. The P&A Cell OIC will designate Red Force Track Managers who are responsible for the overall Red Force CTP maintenance and management. Track Managers will supervise the IAS operators, coordinate and resolve CTP problems with the MSCs' intelligence officers, report system problems to the system administrators, and de-conflict erroneous track data with the MSC's Red Force Track Managers. MSCs will also assign Track

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

Managers to accomplish the same mission at their level. Red Force Track Manager responsibilities include:

(a) Planning Phase

- Identify the systems and units that will be participating in the operation to include G/S-2, other staff elements, adjacent units, and all organic and supporting intelligence, CI and reconnaissance units.
- Diagram the information flow to include auto-forward tables, broadcasts, and manual transmissions.
- Ensure system's time is synchronized.
- Coordinate what type of tracks will be used.
- Ensure IAS training is conducted.
- Ensure C2PC training is conducted.
- Identify what means of communication connectivity will be used to report, troubleshoot, and/or deconflict Red Force track data with subordinate, adjacent, and higher units.
- Identify the chat room(s) and chat server(s) to be used.
- Develop a Red Force Track Matrix and assign responsibilities.
- Determine what maps will need to be loaded into the IAS or IOW (AO-dependent).

(b) Deployment and Set-Up Phase

- Ensure all maps are loaded into the IAS/IOW, to include those of the MSCs.
- Ensure initial Red Force track data is correct, loaded into the IAS, and disseminated throughout the MEF via the S-TDN.

(c) Execution Phase

- Continually monitor the CTP for accuracy at the MEF and the MSCs.
- Communicate with other Red Force Track Managers (subordinate, adjacent, and higher) to ensure Red Force track totals are accurate.
- Ensure MSCs adhere to the Track Matrix and other Red Force track management direction.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- Ensure Red Force tracks are backed up every hour.

- Receive Red Force track change notification from the MSCs.

(2) System Administrators. The ISC, through the CMDO or intelligence systems officer, will designate someone to serve as System Administrator to coordinate, establish, and maintain the network communication link from pre-deployment through redeployment. System Administrators are responsible for defining the network parameters, troubleshooting system related problems, and maintaining system support. MSCs will also assign System Administrators to accomplish the same mission at their level. System Administrator responsibilities include:

(a) Planning Phase

- Identify CIS network requirements.

- Assist Red Force Track Manager with information flow diagrams.

- Identify mail JWICS/SCI-TDN, SIPRNET/S-TDN, and NIPRNET/U-TDN requirements.

- Identify power requirements.

- Identify the IRC chat server(s) IP and alternate IP addresses.

- Create account names (max of eight characters) for both UNIX and NT IOWs.

- Determine how message traffic will enter the system. (e.g., serial or IP address).

- Build guard lists for messages.

(b) Set Up Phase

- Assist with system setup.

- Configure systems on the network (router and host-tables).

- Set up DNS Web browsing for SIPRNET.

- Set up e-mail.

- Set up IRC chat on IAS and IOWs.

- Build communication channel.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- Build DDN host table.
- Set up IOW gateways.
- Configure WAN userids.
- Set system time and synchronize workstations and IOWs.
- Build message profiles (what messages are routed to what accounts).

(c) Execution Phase

- Assist IAS operators with administrative and system related problems.
- Maintain the servers.
- Conduct backups of messages and tracks.
- Monitor network and ensure MSCs capabilities are operational.
- Monitor communications channels to prevent backlog of incoming and outgoing messages.

APPENDIX A

GLOSSARY

Section I

Acronyms

Note: Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.

2. MCRP 5-12C, Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms.

ABC.....airborne corps
A/CSassistant chief of staff
ACEaviation combat
element
ACV.....aircraft cockpit video
ADP.....automated data processing
AFP.....all-source fusion platoon
AFATDS.....advanced field artillery tactical data
system
AIG.....address indicator group
AOarea of operations
AOA amphibious objective area
AOB.....air order of battle
AOI.....area of interest
AOR.....area of
responsibility
ATARS.....advanced tactical airborne reconnaissance system
ATF amphibious task force
ATFICamphibious task force intelligence center
ATO... air tasking order
AWACS.....airborne warning and control system
BDA battle damage assessment
C2 command and control
C4.....command, control, communications, and
computer

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	CAD.....	common address designator
2	CAT.....	crisis action team
3	CCIR..	commander's critical information requirements
4	CD-ROM.....	compact disc-read only
5	memory	
6	CE.....	command element
7	CG.....	commanding
8	general	
9	CHATS.....	CI/HUMINT automated tool set
10	CI.....	counterintelligence
11	CIA	Central Intelligence Agency
12	CIC	combat intelligence center
13	CINC .	commander in chief
14	CIS.....	communications and information
15	systems	
16	CLF....	commander landing force
17	CMD.....	collection
18	management/dissemination	
19	CMDO.....	collection management/dissemination
20	officer	
21	CMS.....	COMSEC material
22	system	
23	COA ..	course of action
24	COC...	combat operations center; current operations center
25	COLISEUM.....	community on-line intelligence system for end users and managers
26	COMINT	communications intelligence
27	COMSEC	communications security
28	CONOPS	concepts of operations
29	CONPLAN	operation plan in concept format, concept plan, contingency plan
30	CONUS.....	continental United States
31	COP.....	common operational picture
32	CPX ...	command post exercise
33	CSS....	combat service support
34	CSSD.....	combat service support detachment
35	CSSE .	combat service support element
36	CTAPS.....	contingency theater automated planning
37	system	
38	CTP.....	common tactical picture
39	DAG.....	DSSCS address group
40	DATEDES.....	date desired
41	DIA	Defense Intelligence Agency
42	DISN.....	defense information systems network
43	DISUM.....	daily intelligence summary

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	DMS.....	defense message
2	system	
3	DOD	Department of Defense
4	DODIPP.....	DOD Intelligence Production Program
5	DP.....	decision point
6	DRAW-D.....	defend, reinforce, attack, withdraw, delay
7	DS.....	direct support
8	DST	direct support team, decision support template
9	DSSCS	defense special security communications system
10	DSVT.....	digital subscriber voice
11	terminal	
12	DZ.....	drop zone
13	e-mail.....	electronic
14	mail	
15	EEFI... ..	essential elements of friendly information
16	ELINT	electronic intelligence
17	EOB	electronic order of battle
18	EW	electronic warfare, early warning
19	FFC.....	force fires
20	center	
21	FFIR.....	friendly force information
22	requirements	
23	FLTSATCOM.....	fleet satellite communication
24	system	
25	FM.....	field manual
26	(Army)	
27	FOC.....	future operations center
28	FSC.....	fire support coordinator
29	FSSG.....	force service support group
30	GCCS.....	global command and control
31	system	
32	GCE	ground combat element
33	GENSER.....	general service
34	GEOINT.....	geographic intelligence
35	GI&S.....	geospatial information and
36	services	
37	GIST.....	geographic intelligence support team
38	GOB.....	ground order of battle
39	GS.....	general support
40	GSP.....	ground sensor platoon
41	HA.....	humanitarian
42	assistance	
43	HET.....	HUMINT exploitation team
44	HF	high frequency

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	HLZ.....	helicopter landing
2	zone	
3	HPT.....	high-payoff target
4	HQ.....	headquarters
5	HST.....	HUMINT support team
6	HUMINT.....	human intelligence, human resources
7	intelligence	
8	HVT.....	high-value target
9	I&W ..	indications and warnings
10	IAS ...	intelligence analysis system
11	ICM	intelligence collection
12	management	
13	ICR ...	intelligence collection requirement
14	IDM	intelligence dissemination
15	management	
16	IDR ...	intelligence dissemination requirement
17	IIP.....	imagery intelligence
18	platoon	
19	IM.....	information
20	management	
21	IMINT	imagery intelligence
22	IMO.....	imagery & mapping officer; information management
23	officer	
24	INFLTREP.....	in-flight
25	report	
26	INMARSAT.....	international maritime satellite system
27	INTELINK	intelligence link
28	INTELINK-S	intelligence link-SECRET
29	INTREP	intelligence report
30	INTSUM.....	intelligence summary
31	IOC	intelligence operations center
32	IOW.....	intelligence-operations
33	workstation	
34	IP.....	internet protocol
35	IPB.....	intelligence preparation of the battlespace
36	IPIR.....	initial photo interpretation report
37	IPL.....	image product library
38	IPM	intelligence production
39	managment	
40	IPR.....	intelligence production requirement
41	IR.....	intelligence requirement
42	IRM	intelligence requirements
43	management	
44	ISC	intelligence support coordinator

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	JAC	joint analysis center
2	JCS	Joint Chiefs of Staff
3	JDISS.	joint deployable intelligence support system
4	JFC.....	joint force commander
5	JIC	joint intelligence center
6	JISE ...	joint intelligence support element
7	JMCIS	joint maritime command information system
8	JSIPS	joint service imagery processing system
9	JTF.....	joint task force
10	JWICS	joint worldwide intelligence communications system
11	KOCSA.....	key terrain, observation and fields of fire, cover & concealment,
12	obstacles,	avenues of approach and
13	mobility corridors	
14	LAN	local area network
15	LF.....	landing force
16	LOC.....	lines of communication
17	LOCE.....	Linked Operational Intelligence Centers Europe
18	LTIOV.....	latest time information of value
19	LZ	landing zone
20	MAG.....	Marine aircraft group
21	MAGTF	Marine Air-Ground Task
22	Force	
23	MARFOR	Marine Corps forces
24	MASINT.....	measurement and signature
25	intelligence	
26	MAW	Marine aircraft
27	wing	
28	MCDP.....	Marine Corps doctrinal
29	publication	
30	MCIA.....	Marine Corps Intelligence
31	Activity	
32	MCISU.....	Marine Corps Imagery Support Unit
33	MCOO.....	mobility corridors and obstacle
34	overlay	
35	MCPP.....	Marine Corps planning process
36	MCRP.....	Marine Corps reference publication
37	MCWP.....	Marine Corps warfighting
38	publication	
39	MEB.....	Marine expeditionary brigade
40	MEF	Marine expeditionary force
41	MEU	Marine expeditionary
42	unit	
43	METT-T.....	mission, enemy, terrain and weather, troops and support available, time
44	available	

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	MEU(SOC).....	Marine expeditionary unit (special operations
2	capable)	
3	MISREP	mission report
4	MOOTW.....	military operations other than war
5	MSC.....	major subordinate
6	command	
7	NA.....	not
8	applicable	
9	NAI.....	named area of interest
10	NEO.....	noncombatant evacuation operation
11	NGO.....	non-governmental organization
12	NIMA.....	National Imagery and Mapping Agency
13	NIPRNET.....	non-secure internet protocol routing network
14	NIST.....	national intelligence support
15	team	
16	NSA.....	National Security
17	Agency	
18	NSTR	nothing significant to report
19	OCAC.....	operations control and analysis
20	center	
21	OOB.....	order of battle
22	OPCON.....	operational control
23	OPLAN.....	operation
24	plan	
25	OPORD.....	operation order
26	OPSEC.....	operations security
27	OSINT.....	open-source intelligence
28	P&A.....	production and
29	analysis	
30	PDA.....	physical damage
31	assessment	
32	PERINTSUM.....	periodic intelligence
33	summary	
34	PIR.....	priority intelligence requirement
35	POC.....	point of contact
36	PR.....	production requirement
37	PVO.....	private volunteer organization
38	Rad Bn.....	Radio Battalion
39	RAOG.....	rear area operations group
40	RFI.....	request for intelligence; request for information
41	ROC.....	reconnaissance operations center
42	RRFI.....	response to request for intelligence
43	RRS.....	remote receive station
44	RRT.....	radio reconnaissance team

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1	SACC.....	supporting arms coordination
2	center	
3	SALUTE.....	size, activity, location, unit, time of observation,
4	equipment	
5	SARC	surveillance and reconnaissance cell
6	SATCOM	satellite
7	communications	
8	SCAMP	sensor control and management platoon
9	SCI ...	sensitive compartmented information
10	SCIF ..	sensitive compartmented information facility
11	SCI-TDN	sensitive compartmented information - tactical data network
12	SCR	single channel
13	radio	
14	SERE.....	survival, evasion, resistance,
15	escape	
16	SI	special
17	intelligence	
18	SIDS.....	secondary imagery dissemination
19	system	
20	SIGINT	signals intelligence
21	SIPRNET.....	SECRET internet protocol router network
22	SOP	standing operating procedure
23	SPMAGTF	special-purpose Marine air-ground task force
24	SPOTREP.....	spot report
25	S-TDN.....	secret-tactical data network
26	SSCC.....	special security communications center
27	SSCE.....	special security communication
28	element	
29	SSCT	special security communication team
30	SSES.....	ship's signals exploitation
31	space	
32	SSO.....	special security officer; special security
33	office	
34	SST.....	SIGINT support team
35	SYSCON	systems control
36	TAI.....	tactical area of interest
37	TACLOG.....	tactical-logistical group
38	TACELINT.....	tactical electronic intelligence report
39	TACREP.....	tactical report
40	TCAC.....	technical control and analysis
41	center	
42	TCO.....	tactical combat operations
43	TDN.....	tactical data network
44	TECHCON	technical control

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1	TEG.....	tactical exploitation group
2	TERPES	tactical electronic reconnaissance processing and evaluation
3	system	
4	TOI.....	time of
5	intelligence	
6	Topo.....	topographic
7	Topo Plt.....	topographic platoon
8	TOR.....	time of report
9	TPC.....	topographic production capability
10	TS-II.....	Trojan Spirit II
11	TTP.....	tactics, techniques, and procedures
12	UAV.....	unmanned aerial
13	vehicle	
14	UHF.....	ultra high
15	frequency	
16	userid.....	user identification
17	U-TDN.....	unclassified tactical data network
18	UTM.....	universal transverse mercator
19	VHF	very high frequency
20	VMAQ	Marine tactical electronic warfare squadron
21	VMU.....	Marine unmanned aerial vehicle
22	squadron	
23	VTC.....	video
24	teleconference	
25	WAN	wide area network
26	WMD.....	weapons of mass
27	destruction	
28	www.....	world wide web
29	WSV.....	weapons systems video

Section II

Definitions

Note: Definitions of military terms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official definitions of military terms:

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.

2. MCRP 5-12C, Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms.

A

all-source intelligence -- Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the finished intelligence. (Joint Pub 1-02)

amphibious objective area - A geographical area, delineated in the initiating directive, for purposes of command and control within which is located the objective(s) to be secured by the amphibious task force. This area must be of sufficient size to ensure accomplishment of the amphibious task force's mission and must provide sufficient area for conducting necessary sea, air, and land operations. Also called AOA. (Joint Pub 1-02)

area of interest - That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (Joint Pub 1-02)

area of operations - An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their mission and protect their force. Also called AO. (Joint Pub 1-02)

B

basic intelligence - Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

battle damage assessment - 1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (Joint Pub 1-02) 2. The timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 5-12C)

battlespace - All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

branch(es) - A contingency plan or course of action (an option built into the basic plan or course of action) for changing the mission, disposition, orientation, or direction of movement of the force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions. See also sequels. (MCRP 5-12C)

C

collate - 1. The grouping together of related items to provide a record of events and facilitate further processing. 2. To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing phase of the intelligence cycle. (Joint Pub 1-02)

collection - The gathering of intelligence data and information to satisfy the identified requirements. (MCWP 5-12C)

collection agency - Any individual, organization, or that has access to sources of information and the capability of collecting information from them. (Joint Pub 1-02)

collection asset - A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (Joint Pub 1-02)

collection management - 1. The process of converting intelligence requirements into collection requirements, establishing priorities, and tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (Joint Pub 1-02)

collection manager - An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. Also called CM. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

collection plan - A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (Joint Pub 1-02)

combat data - Data derived from reporting by operational units. (MCWP 5-12C)

combat information – Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (Joint Pub 1-02)

combatant command - A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (Joint Pub 1-02)

combined operation - An operation conducted by forces of two or more allied nations acting together for the accomplishment of a single mission. (Joint Pub 1-02)

command and control - 1. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02) 2. The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

commander's critical information requirements - Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirement; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent - A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

commander's planning guidance - Directions and/or instructions which focus the staff's course of action development during the planning process. Also called CPG. (MCRP 5-12C)

communications intelligence - Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 2-0)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

communications security - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (Joint Pub 1-02)

component command - One of the subordinate organizations that constitute a joint force. Normally a joint force is organized with a combination of Service and functional components. The Service component command consists of its Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command, or further assigned to a subordinate unified command or joint task force. (Joint Pub 1-02)

coordination - The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence - 1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on the behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Joint Pub 1-02) 2. Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCRP 5-12C)

crisis action planning - The time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs. (Joint Pub 1-02)

critical information - Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02)

critical intelligence - Intelligence which is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/ actual enemy. It includes but is not limited to the following:

- Strong indications of the imminent outbreak of hostilities of any type (warning of attack)
- Aggression of any nature against a friendly country
- Indications or use of nuclear-biological-chemical weapons (target)
- Significant events within potential enemy countries that may lead to modification of nuclear strike plans. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

critical node - An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. (Joint Pub 1-02)

critical vulnerability - An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called CV. (MCRP 5-12C)

D

daily intelligence summary - A report prepared in message format at the joint force headquarters that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The "as of" time for the information, content, and submission time for the report will be specified by the joint force commander. Also called DISUM. (Joint Pub 1-02)

data - Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning or insight is or might be assigned. (Joint Pub 1-02)

database - Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (Joint Pub 1-02)

database replication - Process by which like databases reflect commonality in information and timeliness of that information. (MCRP 5-12C)

debriefing - Interviewing of an individual who has completed an intelligence or reconnaissance assignment or who has had knowledge, whether through observation, participation, or otherwise, of operational intelligence significance. (MCRP 5-12C)

decentralized control - In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

decision point - An event, area, or point in the battlespace where and when the friendly commander will make a critical decision. Also called DP. (MCRP 5-12C)

deliberate planning - A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

deliberate targeting - The methodical identification, compilation, and analysis of potential fixed and semifixed targets followed by the decision of which potential targets will be attacked, when, and/or by what weapon and ordnance. It is practiced primarily during the planning phase of an operation, when planning for an attack, or when the tempo of combat is slow. (MCRP 5-12C)

descriptive intelligence - Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligence*, which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment - 1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (Joint Pub 1-02)

direction finding - A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receive or ancillary equipment. (Joint Pub 1-02)

direct support - A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (Joint Pub 1-02)

dissemination - Conveyance of intelligence to users in a suitable form. (Joint Pub 1-02)

dissemination management - Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

E

electronic intelligence - Technical and geolocational intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (Joint Pub 1-02)

electronic reconnaissance - The detection, identification, evaluation, and location of foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

electronic warfare - Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. Also called EW. (Joint Pub 1-02)

essential elements of friendly information - 1. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (Joint Pub 1-02) 2. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence - Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. See also **descriptive intelligence**. (MCRP 5-12C)

F

fires - The effects of lethal or non lethal weapons.

force protection - Security programs designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, and supported by intelligence, counterintelligence, and other security programs. (Joint Pub 1-02)

force reconnaissance company - A unit whose mission is to conduct preassault and deep postassault reconnaissance operations in support of a landing force and its subordinate elements. (MCRP 5-12C)

friendly force information requirements - Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

fusion - In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (Joint Pub 1-02)

fusion center - In intelligence usage, a physical location to accomplish fusion. It normally has sufficient intelligence automated data processing capability to assist in the process. (Joint Pub 1-02)

future operations section - 1. In MAGTF operations, a section normally under the staff cognizance of the G-3 which focuses on planning/producing new fragmentary orders or the next change of major subordinate command mission; this section forms and leads the integrated planning effort with a planning horizon of 72-120 hours out. It develops branch plans and

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

sequels. 2. In Marine aviation, that portion of the tactical air command center and aviation combat element commander's battlestaff responsible for the detailed planning and coordination of all future air operations conducted by the aviation combat element in support of the Marine air-ground task force. The future operations section plans for and publishes the next air tasking order(s) (normally a 48/72-hour period). (MCRP 5-12C)

G

general military intelligence - Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or allied military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilian C4 systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) Also called GMI. (Joint Pub 1-02)

general support - That support which is given to the supported force as a whole and not to any particular subdivision thereof. (Joint Pub 1-02)

geographic coordinates - The quantities of latitude and longitude which define the position of a point on the surface of the earth with respect to the reference spheroid. (Joint Pub 1-02)

geographic intelligence - The process of collecting, organizing, analyzing, synthesizing, disseminating and utilizing geospatial information and services (GI&S) with regards to the military aspects of the terrain. Also called GEOINT. GEOINT is the integration and analysis of all-source geospatial information in support of specific Marine Corps operations. The analysis is focused on a specific mission and includes intensification of information detail and resolution to meet tactical requirements. GEOINT analysis is focused on the intelligence preparation of the battlespace (IPB) process and addresses key terrain, observation & fields of fire, cover & concealment, obstacles, avenues of approach & mobility corridors. This analysis is commonly referred to as KOCO for easy reference.

geospatial information and services - The concept for collection, information extraction, product generation, storage, dissemination, and utilization of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data. These data are used for military planning, training, and operations including aeronautical, nautical and land navigation, as well as mission planning, mission rehearsal, modeling and simulation and precise targeting. It also includes the evaluation and analysis of topographic, hydrophobic, littoral, or aeronautical features for their effect on military planning, operations and intelligence. This analysis could also include the development of a commander's visualization and preparation of the battlespace. It may be presented in the

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

form of printed maps, charts and publications; in digital simulation and modeling databases; in photographic form; or in digital form. Also called GI&S. (Nominated for inclusion in Joint Pub 1-02)

global sourcing - A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

H

helicopter landing zone - A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called HLZ. (Joint Pub 1-02)

high-payoff target - A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through wargaming, which must be acquired and successfully attacked for the success of the friendly commander's mission. Also called HPT. (Joint Pub 1-02)

high-value target - A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called HVT. (Joint Pub 1-02)

human intelligence - 1. A category of intelligence derived from information collected and provided by human sources. (Joint Pub 1-02) 2. In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called HUMINT. (Joint Pub 1-02)

humanitarian assistance - Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have primary responsibility for providing humanitarian assistance. Also called HA. (Joint Pub 1-02)

hydrography - The science which deals with the measurement and description of the physical features of the oceans, seas, lakes, rivers, and their adjoining coastal areas, with particular reference to their use for navigational purposes. (Joint Pub 1-02)

I

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

imagery exploitation - The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (Joint Pub 1-02)

imagery intelligence - Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (Joint Pub 1-02)

imagery interpretation - The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. (Joint Pub 1-02)

indications and warning - Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events. Also called I&W. (Joint Pub 1-02)

information - 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

information report - Report used to forward raw information collected to fulfill intelligence requirements. (Joint Pub 1-02)

information requirements - Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (Joint Pub 1-02)

information exchange requirement - The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement. Also called IER. (MCRP 5-12C)

integration - A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (Joint Pub 1-02)

intelligence - 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation,

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

analysis, or understanding. (Joint Pub 1-02) 3. Knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence annex - A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (Joint Pub 1-02)

intelligence cycle - The process by which information is converted into intelligence and made available to users. (Joint Pub 2-01)

intelligence data - Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline - A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open source intelligence. (Joint Pub 1-02)

intelligence estimate - The appraisal, expressed in written, oral, or graphic form, of available intelligence relating to a specific situation or condition with a view to determine the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

intelligence operations - The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Joint Pub 1-02)

intelligence preparation of the battlespace - 1. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (Joint Pub 1-02) 2. In Marine Corps usage, the systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence report - A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (Joint Pub 1-02)

intelligence requirement - 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02) 2. In Marine Corps

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IR. (MCRP 5-12C)

J

joint deployable intelligence support system - A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (Joint Pub 1-02)

joint force - A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint intelligence center - The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (Joint Pub 1-02)

joint intelligence support element - A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (Joint Pub 1-02)

joint operations - A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (Joint Pub 1-02)

joint task force - A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub unified commander, or an existing joint task force commander. Also called JTF. (Joint Pub 1-02)

joint worldwide intelligence communications system - The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multi-point information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Joint Pub 1-02)

L

line of communication - A route, either land, water, and/or air, which connects an operating military force with a base of operations and along which supplies and military forces move. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

M

Marine Corps planning process - A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

measurement and signature intelligence - 1. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT.

military operations other than war - Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other elements of national power and occur before, during, and after war. Also called MOOTW. (Joint Pub 1-02)

multinational operations - A collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance. (Joint Pub 1-02)

N

named area of interest - A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

national intelligence support team - A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (Joint Pub 2-01)

near real time - Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

noncombatant evacuation operations - Operations directed by the Department of State, the Department of Defense, or other appropriate authority whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or the United States. Also called NEO. (Joint Pub 1-02)

O

open-source intelligence - Information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operational architecture - A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanged requirements. Also called OA. (MCRP 5-12C)

operational control - Transferable command authority which may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations; normally this authority is exercised through the service component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (Joint Pub 1-02)

operations control and analysis center - Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelligence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called OCAC. (MCRP 5-12C)

order of battle - The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (Joint Pub 1-02)

P

priority intelligence requirements - 1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 PIR. (Joint Pub 1-02) 2. An intelligence requirement associated with a decision that will critically
2 affect the overall success of the command's mission. (MCRP 5-12C)

3
4 **production** - The conversion of information into intelligence through the integration, analysis,
5 evaluation, and interpretation of all-source data and the preparation of intelligence products in
6 support of known or anticipated user requirements. Production is a process of synthesis -- the
7 most important action in developing usable intelligence for the commander. (MCWP 2-1)

8
9 **production management** - Encompasses determining the scope, content, and format of each
10 product, developing a plan and schedule for the development of each product, assigning priorities
11 among the various production requirements, allocating processing, exploitation, and production
12 resources, and integrating production efforts with collection and dissemination. (MCRP 5-12C)

R

13
14
15
16 **reach back** - The ability to exploit resources, capabilities, expertise, etc. not physically located in
17 the theater or a joint area of operations, when established. (MCRP 5-12C)

18
19 **reactive targeting** - The method used for targeting target of opportunity. It is used when time
20 and situation do not allow for deliberate targeting; i.e., during an attack, when defending against
21 an attack, or upon discovery of the location of a target such as a radio jammer, tank, or
22 antiaircraft weapon. (MCRP 5-12C)

23
24 **request for information** - Any specific time-sensitive ad hoc requirement for intelligence
25 information or products to support an ongoing crisis or operation not necessarily related to
26 standing requirements or scheduled intelligence production. A request for information can be
27 initiated to respond to operational requirements and will be validated in accordance with the
28 theater commander's procedures. (Joint Pub 1-02)

S

29
30
31
32
33 **SECRET internet protocol router network** - Worldwide SECRET level packet switch network
34 that uses high-speed internet protocol routers and high-capacity Defense Information Systems
35 Network circuitry. Also called SIPRNET. (Joint Pub 1-02)

36
37 **sensitive compartmented information** - All information and materials bearing special
38 intelligence community controls indicating restricted handling within present and future
39 community intelligence collection programs and their end products for which community
40 systems of compartmentation have been or will be formally established. Also called SCI. (Joint
41 Pub 1-02)

42
43 **sensitive compartmented information facility** - A restricted access facility providing SCI
44 communications, processing, and storage. Also called SCIF. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

sensor data - Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

signals intelligence - A category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumental signals intelligence, however transmitted. Also called SIGINT. (Joint Pub 1-02)

situational awareness - Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

surveillance and reconnaissance cell - Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (MCRP 5-12C)

T

tactical intelligence -- 1. Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02) 2. Tactical intelligence concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

target - A geographical area, complex, or installation planned for capture or destruction by military forces. (Joint Pub 1-02)

target analysis - An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (Joint Pub 1-02)

target area of interest - The geographical area or point along a mobility corridor where successful interdiction will cause the enemy to either abandon a particular course of action or require him to use specialized engineer support to continue, where he can be acquired and engaged by friendly forces. Not all target areas of interest will form part of the friendly course of action; only target areas of interest associated with high-payoff targets are of interest to the staff. These are identified during staff planning and wargaming. Target areas of interest differ from engagement areas in degree. Engagement areas plan for the use of all available weapons. Target areas of interest might be engaged by a single weapon. Also called TAI. (MCRP 5-12C)

target intelligence - Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (Joint Pub 1-02)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

tempest – An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (Joint Pub 1-02)

terrain analysis - The collection, analysis, evaluation, and interpretation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (Joint Pub 1-02)

terrain study - An analysis and interpretation of natural manmade features of an area, their effects on military operations, and the effect of weather and climate on those features. (Joint Pub 1-02)

W

warfighting functions - The six mutually supporting military activities integrated in the conduct of all military operations are:

1. **Command and control** -- the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.
2. **Maneuver** -- the movement of forces for the purpose of gaining an advantage over the enemy.
3. **Fires** -- those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.
4. **Intelligence** -- knowledge about the enemy or the surrounding environment needed to support decisionmaking.
5. **Logistics** -- all activities required to move and sustain military forces.
6. **Force protection** -- actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. (MCRP 5-12C)

Appendix B

REFERENCES

Joint Publications (Joint Pubs)

- 1-02 Department of Defense Dictionary of Military and Associated Terms
- 2-0 Doctrine for Intelligence Support to Joint Operations
- 2-01 Joint Intelligence Support to Military Operations
- 2-01.1 Intelligence Support to Targeting
- 2-01.2 Counterintelligence Support
- 2-02 National Intelligence Support to Joint Operations
- 2-03 Geospatial Information
- CJCSI 3151.01 Global Command and Control System Common Operational Picture Reporting Requirements

Marine Corps Doctrinal Publications (MCDPs)

- 1 Warfighting
- 1-1 Strategy
- 1-2 Campaigning
- 1-3 Tactics
- 2 Intelligence
- 3 Expeditionary Operations
- 4 Logistics
- 5 Planning
- 6 Command and Control

Marine Corps Warfighting Publications (MCWPs)

- 2-1 Intelligence Operations
- 2-11 MAGTF Intelligence Collection (draft)
- 2-12 MAGTF Intelligence Analysis and Production (draft)
- 2-12.1 Geographic Intelligence (draft)
- 2-14 Counterintelligence (draft)
- 2-15.1 Remote Sensor Operations
- 2-15.2 Signals Intelligence
- 2-15.3 Ground Reconnaissance (draft)
- 2-15.4 Imagery Intelligence (draft)
- 2-15.5 Interrogator-Translator Operations (draft)

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 3-2 Aviation Operations (draft)
- 2 5-1 Marine Corps Planning Process
- 3 6-2 MAGTF Command and Control (draft)
- 4 6-22 Communications and Information Systems
- 5 6-23 Information Management (draft)
- 6
- 7

Marine Corps Reference Publications (MCRPs)

- 9
- 10 2-11A RECCE-J (MCRP 2-2.1/ALSA PUB)
- 11 2-11B Joint STARS (ALSA PUB)
- 12 2-12A IPB (FMFRP 3-13-2/FM 34-130)
- 13 2-15.3A Recon Patrol Leader's Planning Handbook
- 14 2-15.3B Reconnaissance Reports and Formats
- 15 5-12A Operational Terms and Graphics
- 16 5-12C Marine Corps Supplement to the Department of Defense Dictionary
- 17 of Military and Associated Terms
- 18 5-12D Organization of Marine Corps Forces
- 19 6-23A Joint Task Force Information Management
- 20
- 21

Appendix C

Intelligence Estimate Format

This appendix provides the format for an intelligence estimate to an operations order, written from the perspective of a MAGTF. The first example is for an intelligence estimate in support of conventional combat operations. The second example provides the format for an intelligence estimate in support of MOOTW.

OF ISSUE

Copy no. __ of __ copies
Issuing headquarters PLACE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (Number)

Ref : (a) Maps and Charts
(b) Other pertinent intelligence documents and online databases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. MISSION. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. CHARACTERISTICS OF THE AREA OR OPERATIONS. (State conditions which exist and indicate the effect of these conditions on enemy capabilities and the assigned mission. Assess the estimated effects of these conditions on both enemy and friendly capabilities and operations.)

a. Military Geography

(1) Topography

(2) Drainage

(3) Vegetation

(4) Surface materials

(5) Military aspects of terrain

(6) Effects of terrain on enemy and friendly capabilities and operations

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

b. Hydrography

(1) Coastline description

(2) Hydrographic conditions

(a) Surf

(b) Tides

(c) Currents

(3) Beaches

(4) Effects of hydrography on enemy and friendly capabilities and operations

c. Climate and Weather

(1) Type and characteristics

(2) Temperature

(3) Precipitation

(4) Visibility

(5) Winds

(6) Light Data

(7) Flight conditions

(8) Effects of weather on enemy and friendly capabilities and operations

d. Transportation

(1) Airfields

(2) Helicopter landing zones

(3) Port facilities

(4) Roads

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

(5) Railroads

(6) Inland waterways

(7) Effects of transportation on enemy and friendly capabilities and operations

e. Civilian Telecommunications and Media

(1) International

(2) Domestic

(3) Mass communications -- types, capabilities, key facilities

(a) Radio

(b) Television

(c) Print media

(4) Effects of telecommunications and media on enemy and friendly capabilities and operations

f. Economics and Infrastructure

(1) General economic activity and conditions (industry, public works and utilities, finance, banking, agriculture, trades and professions, labor force, etc.)

(2) Monetary system

(3) Power and utilities

(4) POL facilities

(5) Effects of economics and infrastructure on enemy and friendly capabilities and operations

g. Politics

(1) Political system and climate

(2) Local political conditions

(3) Local political leaders

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

(4) Policy and attitudes towards the U.S. and the U.S. military

(5) Effects of political situation on enemy and friendly capabilities and operations

h. Sociology

(1) Cities and towns

(2) Population and distribution of area and of key cities and towns

(3) Ethnic composition

(4) Languages

(5) Religions

(6) Customs and norms

(7) Social institutions and attitudes

(8) Effects of sociological situation on enemy and friendly capabilities and operations

i. Health and Medical

(1) Food supply

(2) Water supply

(3) Diseases and other medical problems

(4) Plant and animal hazards

(5) Sanitation

(6) Medical facilities

(7) Effects of health and medical situation on enemy and friendly capabilities and operations

3. ENEMY MILITARY SITUATION

a. Ground Forces

(1) Composition, organization and strengths. (Describe the structure of enemy forces [i.e., order of battle] and describe unusual organizational features, identity, etc. State the number

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

1 and size of enemy units in and others available for use in the area of operations. Provide
2 estimated combat effectiveness of enemy forces.)

3
4 (2) Disposition, locations, movements and activities. (Describe the geographic location
5 and latest known activities of enemy forces, including command and control facilities, fire
6 support elements, and other key combat support forces.)

7
8 (a) Committed forces. (For ground forces, include all units currently in contact or
9 with which contact is imminent within the unit's AO, regardless of the specific friendly course of
10 action. For amphibious or forcible entry operations, committed forces would be those which
11 could immediately engage friendly units at their point of insertion. All fire support assets within
12 range are normally considered committed, regardless of subordination. Conventional military
13 forces are referred to by numbers of unit types (armor, infantry, etc.) two echelons below the
14 friendly unit. Guerrilla or insurgent forces are expressed in terms of total numbers of personnel
15 and fire support weapons.

16
17 (b) Reinforcements. (Describe the enemy's reinforcement capabilities in terms of
18 possible forces and weapons that can react in time to affect the accomplishment of the mission.
19 Factors to be considered include time available to react, terrain, weather, road and rail nets,
20 transportation, replacements, and possible aid from sympathetic or participating neighbors.)

21
22 (3) Weapons and equipment. (Describe the operational capabilities and technical
23 characteristics of major items of equipment in the enemy's inventory.)

24
25 (4) Command and control

26
27 (a) Organization

28
29 (b) Key C2 nodes

30
31 (c) Communications and information systems

32
33 (5) Logistics. (Describe levels of supply, resupply ability, and capacity of beaches, ports,
34 roads, railways, airfields, and other facilities to support supply and resupply. Consider
35 transportation, hospitalization and evacuation, military construction, labor resources, and
36 maintenance of combat equipment, etc.).

37
38 (6) Training, tactics, operating patterns

39
40 (7) Capabilities and effectiveness

41
42 b. Naval Forces

43
44 (1) Composition, organization and strengths

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

c. Air Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

d. Air Defense Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

e. Paramilitary and Security Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

f. Command and Control Warfare Capability

(1) Intelligence, counterintelligence, and reconnaissance capabilities

(2) Electronic warfare capabilities

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(3) Psychological warfare capabilities

(4) Deception capabilities

(5) Operational security capabilities

g. Nuclear, Biological and Chemical Capabilities

h. Night Combat Capabilities

i. Unconventional Warfare Capabilities (guerrilla, subversion, sabotage, terrorism)

4. CAPABILITIES AND ANALYSIS. (List separately each enemy capability which can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering all applicable factors from paragraphs 2 and 3, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission. The term "capabilities" includes not only the general courses of action open to the enemy (i.e. attack, defend, withdraw, etc.), but also the particular courses of action possible under each general course of action. These COAs should correspond exactly to the enemy COA models developed during step 4 of IPB.)

5. CONCLUSIONS AND VULNERABILITIES. (Conclusions resulting from discussion in paragraph 4. Include: enemy centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

/s/ _____

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 TABS (omit or add other tabs as required)
- 2
- 3 A. Tactical Study of Terrain
- 4
- 5 B. Beach Studies
- 6
- 7 C. Climatology Study
- 8
- 9 D. Airfield Studies
- 10
- 11 E. HLZ and DZ Studies
- 12
- 13 F. Port Studies
- 14
- 15 G. Lines of Communications Study
- 16
- 17 H. Order of Battle Study
- 18
- 19
- 20
- 21

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

MOOTW ESTIMATE FORMAT

Copy no. __ of __ copies
Issuing headquarters
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (Number)

Ref : (a) Maps and Charts
(b) Other pertinent intelligence documents and online databases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. **MISSION.** (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. **CHARACTERISTICS OF THE AREA OR OPERATIONS.** (Discuss characteristics of the host nation (HN), the area, and their probable effects upon the threat(s), the mission force, and the host government.)

a. **Geography**

(1) Strategic location.

(a) Neighboring countries and boundaries.

(b) Natural defenses including frontiers.

(c) Points of entry and strategic routes.

(2) Size and dimensions.

(3) Relief.

(4) Beach Data.

(5) Hydrography.

(a) Coastal.

(b) Lakes.

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

(c) Rivers.

(6) Land use.

(7) Geological basics.

(8) Vegetation

(9) Water sources.

(10) Natural foods.

(11) Population centers.

(12) Wildlife.

b. Climate and Weather

(1) Type and characteristics.

(2) Temperature.

(3) Precipitation.

(4) Visibility.

(5) Winds.

(6) Light Data.

(7) Flight conditions.

(8) Seasonal effects of weather on terrain and visibility.

c. Demographics

(1) History.

(2) Ethnic composition.

(3) Languages.

(4) Social system.

(5) Education.

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

(6) Living conditions.

(7) Cultural customs.

(8) Religions.

(9) Taboos.

(10) Grievances.

(11) Psychology (Behavior patterns and motivating factors.)

d. Transportation

(1) Airfields

(2) Helicopter landing zones

(3) Port facilities

(4) Roads

(5) Railroads

(6) Inland waterways

e. Civilian Telecommunications and Media

(1) International

(2) Domestic

(3) Mass communications -- types, capabilities, key facilities

(a) Radio

(b) Television

(c) Print media

MCWP 2-13, MAGTF Intelligence Dissemination
AUTHOR'S DRAFT

6/5/00

1
2 f. Politics (Address existing situation, effects on threat(s), HN, and mission force.)
3

4 (1) National government.
5

6 (a) Structure.
7

8 (b) Regional and/or international role.
9

10 (c) Degree of popular support.
11

12 (2) Political parties (Both sanctioned and unsanctioned.)
13

14 (3) Foreign dependence or alliances.
15

16 (4) Controls and restrictions.
17

18 (5) Legal system (both civil and religious.)
19

20 (6) Grievances.
21

22 g. Economics (Address existing situation, effects on threat(s), HN, and mission force.)
23

24 (1) Current value of currency and wage scales.
25

26 (2) Financial structure to include national and international.
27

28 (3) Foreign dependence.
29

30 (a) Assistance programs.
31

32 (b) Foreign-owned businesses and enterprises in country.
33

34 (c) Trade agreements.
35

36 (4) Agriculture and domestic food supply.
37

38 (5) Natural resources and degree of self-sufficiency.
39

40 (6) Industry.
41

42 (a) Types.
43

44 (b) Production levels.
45

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

- (c) Consumer demands.
- (d) Unions.
- (7) Black market and illicit trades (drugs, weapons, etc.)
- (8) Technology.
- (a) Capabilities.
- (b) Expertise.
- h. Health and Medical
 - (1) Food supply
 - (2) Water supply
 - (3) Diseases and other medical problems
 - (4) Plant and animal hazards
 - (5) Sanitation
 - (6) Medical facilities
- 3. THREATS (Note: For each category of threat (except medical/environmental and natural disasters) discuss organization and leadership (to include composition); strength and dispositions; recent and present significant activities, strengths and weaknesses; and relationships with other threat categories.)
 - a. Conventional.
 - b. Insurgent.
 - c. Clans, Tribes, or Factions.
 - d. Terrorist.
 - e. Drug producers or traffickers
 - f. Criminal organizations.
 - g. Third-party nation and external.

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

h. Civil unrest

i. Medical and environmental.

j. Natural disasters.

4. CAPABILITIES AND ANALYSIS (List current threat capabilities and discuss in regard to probability of adoption)

a. Enumeration. (Includes what, where, when, and how, for each category of threat.)

(1) Basic capabilities.

(a) Conventional.

(b) Insurgent.

(c) Clans, Tribes, or Factions.

(d) Terrorist.

(e) Drug producers or traffickers

(f) Criminal organizations.

(g) Third-party nation and external.

(h) Civil unrest

(i) Medical and environmental.

(j) Natural disasters.

(2) Supporting capabilities. (Includes intelligence, security, recruitment, organization, training, finance, and logistics.)

(a) Conventional.

(b) Insurgent.

(c) Clans, Tribes, or Factions.

(d) Terrorist.

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

(e) Drug producers or traffickers

(f) Criminal organizations.

(g) Third-party nation and external.

(h) Civil unrest

(i) Medical and environmental.

(j) Natural disasters.

b. Analysis and Discussion. (Includes all evidence supporting or rejecting the adoption of each capability.)

5. HN SECURITY

a. Situation. (For each sub-paragraph describe organization and leadership; strength and disposition; recent and present significant activities; and strengths and weaknesses.)

(1) Public order/internal security forces.

(2) Armed forces.

(3) External support forces an dependency. (Regional peacekeeping, foreign forces, mercenaries, etc.)

b. Capabilities. (What, where, when, how for both basic capabilities and supporting capabilities.)

(1) Public order/internal security forces.

(2) Armed forces.

(3) External support forces an dependency.

c. Analysis and discussion.

6. FRIENDLY AND NEUTRAL THIRD-PARTY

a. Situation. (For each sub-paragraph, as defined in 5.a.)

(1) Embassies and consulates.

(2) Military.

MCWP 2-13, *MAGTF Intelligence Dissemination*
AUTHOR'S DRAFT

6/5/00

(3) Business interests.

(4) NGO/PVO.

b. Capabilities. (As defined in 5.b.)

(1) Embassies and consulates.

(2) Military.

(3) Business interests.

(4) NGO/PVO.

c. Analysis and discussion.

7. CONCLUSIONS and VULNERABILITIES

a. Effects of the operational environment. (State total effect of the AO upon COAs.)

b. Probable threat COAs. (Listed in order of relative probability of adoption.)

c. Threat vulnerabilities. (List exploitable threat vulnerabilities.)

TABS (as necessary)

Appendix D

Intelligence Briefing Formats

This appendix provides basic formats for the following common types of intelligence briefings: Intelligence Information (or Orientation) Brief; Intelligence Estimate of Supportability Brief; Mission/Target Intelligence Brief; Intelligence Decision Brief; and Intelligence Confirmation Brief. These formats should be modified for use as appropriate, in accordance with the situation and command SOPs and orders.

BASIC INTELLIGENCE INFORMATION
(ORIENTATION) BRIEFING FORMAT

1. INTRODUCTION
2. GENERAL/SPECIAL SITUATION
3. MILITARY GEOGRAPHY (AS IT IMPACTS OPS IN THE AO)
 - a. Topography
 - (1) Rivers & Streams
 - (2) Mountains
 - (3) Obstacles
 - (4) Vegetation
 - b. Hydrography
 - (1) Rivers
 - (2) Oceans & Beaches
 - (3) Ports
 - c. Terrain Effects (KOCOA)
 - d. Weather/Climate
 - (1) Winds
 - (2) Precipitation

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

(3) Temperatures

(4) Weather Effects

(5) Astronomical Data

4. TRANSPORTATION

a. LOC Trafficability (Railways & Roads)

b. Avenues of Approach

c. Bridges (Type & Capability)

d. Airfields (Existing/Expeditionary)

e. Time/Distance Factors

5. MILITARY FORCES IN THE AOA

a. Ground Forces

(1) Composition

(2) Disposition (Committed forces, Reinforcements, Unit boundaries)

(3) Strength

(4) Key Equipment

(5) Doctrinal & Situational Templates

(6) Logistics

(7) Morale

b. Air Forces

(1) Composition

(2) Disposition (Committed forces, Reinforcements)

(3) Strength

(4) Key Equipment

(5) Logistics

(6) Morale

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

c. Air Defense Forces

(1) Composition

(2) Disposition

(3) Strength

(4) Key Equipment

(5) Doctrinal & Situational Templates

(6) Logistics

(7) Morale

d. Naval Forces

(1) Composition

(2) Disposition (Committed forces, Reinforcements)

(3) Strength

(4) Key Equipment

(5) Logistics

(6) Morale

6. NBC

a. Composition

b. Disposition

c. Strength

d. Key Equipment

e. Doctrinal & Situational Templates

7. INTELLIGENCE & COUNTERINTELLIGENCE

8. UNCONVENTIONAL WARFARE

a. Guerilla Warfare

b. Sabotage

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

c. Subversion

d. Psychological Operations

9. ANALYSIS OF CAPABILITIES

a. Centers of Gravity (Operational & Tactical)

b. Strengths

c. Critical Vulnerabilities

d. Force Correlation (Operational & Tactical)

10. COURSES OF ACTION

a. DRAW-D

b. Most Likely (Short/Long Term) (Operational/Tactical)

c. Most Dangerous (To Friendly Forces) (Operational/Tactical)

11. HISTORICAL PERSPECTIVES

12. COLLECTION AND PRODUCTION CAPABILITIES

INTELLIGENCE ESTIMATE OF SUPPORTABILITY
BRIEFING FORMAT

The single generic staff estimate format, shown below, standardizes the way staff members develop and give staff estimates. The G/S-2 (with input assistance from all staff members) will still conduct and disseminate the initial intelligence preparation of the battlefield as a separate product.

1. MISSION. Restated mission resulting from the mission analysis.

2. SITUATION AND CONSIDERATIONS

A. CHARACTERISTICS OF AREA OF OPERATION

(1) Weather. How will different military aspects of weather affect specific staff area of concern and resources?

(2) Terrain. How will aspects of the terrain affect specific staff areas of concern and resources?

(3) Other pertinent facts. Analyses of political, economic, sociological, psychological, and environmental infrastructure, as they relate to the area.

B. ENEMY FORCES. Enemy dispositions, composition, strength, capabilities, and COAs as they affect specific staff area of concern.

C. FRIENDLY FORCES

(1) Friendly courses of action

(2) Current status of organic intelligence, CI and reconnaissance units

(3) Current status of other supporting or external intelligence, CI and reconnaissance units and resources

(4) Key considerations or evaluation criteria used for COA intelligence supportability estimate

D. ASSUMPTIONS

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

3. INTELLIGENCE SUPPORTABILITY (address each of the below for each friendly COA under consideration)

PURPOSE/AGENDA

- Orientation
- PIRs and IRs (By Phase)
- Assets Available
- Intelligence, CI and Reconnaissance Units Task Organization and C2 Relationships

INTELLIGENCE CONCEPT OF OPERATIONS

- Present key collection and production plans' information
(By estimated threat COAs or by phase for each intelligence asset)
- PIRs/IRs and key indicators
- NAI's assigned
- Movement to/from NAI, time on target, insert time and means, and any other relevant intelligence operational in formation
- Security
- Recovery/Link up/Extract plan; or intelligence operations hand-off plan
- Timeline

COMMUNICATIONS PLAN

- Use Connectivity Diagram
- Communication Schedule: routine and time-sensitive
- Nets used: primary and all specified alternates
- Other communication and dissemination information
(e.g., plan to shift reporting recipient from one command echelon to another)
- No Comm Plan

4. ANALYSIS OF FRIENDLY INTELLIGENCE SUPPORTABILITY

(Summarize, compare and contrast information provided for all friendly COAs under consideration and principal advantages and disadvantages for each. Keep focus on PIRs and IRs. Ensure any deficiencies or gaps are clearly identified.)

5. CONCLUSIONS AND RECOMMENDATIONS

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

**MISSION / TARGET ANALYSIS
INTELLIGENCE BRIEFING FORMAT**

1. ORIENTATION AND INTRODUCTION

- a. Introduce Staff
- b. Orientation to map
- c. Mission

2. AREA OF OPERATIONS

- a. Weather
 - (1) Existing Situation
 - (2) Effects on Enemy Courses of Action
 - (3) Effects on Friendly Courses of Action
- b. Terrain
 - (1) Existing Situation (KOCOA)
 - (2) Effects on Enemy Courses of Action
 - (3) Effects on Friendly Courses of Action
- c. Other Characteristics
 - (1) Existing Situation
 - (2) Effects on Enemy Courses of Action
 - (3) Effects on Friendly Courses of Action

3. ENEMY SITUATION

- a. Disposition
- b. Composition
- c. Strength
 - (1) Committed Forces
 - (2) Reinforcements
 - (3) Intelligence, espionage, sabotage, terrorism
 - (4) Air
 - (5) Artillery
 - (6) NBC
 - (7) Other threat functions or key capabilities, as appropriate
- d. Recent and Current Significant Activities
- e. Critical Vulnerabilities and Weaknesses

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1
2
3 4. ENEMY CAPABILITIES
4

- 5 a. Mission
6 b. Enemy desired end state
7 c. COAs
8 I. Most Likely
9 II. Most Dangerous
10 III. Other COAs
11

12 5. PIRs

- 13 a. Intelligence Operations Status & Initial Collection, Production, & Dissemination Plans
14 I. Assets tasked
15 II. Start and stop time
16 III. PIRs supported
17 b. Recommend for Commander's approval
18

19 6. CONCLUSIONS
20

- 21 a. Effects of Intelligence Considerations on Friendly Operations
22 b. Effects of AO on Own COAs
23 c. Probably Enemy COA and Reactions
24 d. Enemy Vulnerabilities
25

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

INTELLIGENCE DECISION BRIEFING FORMAT

1
2
3
4 1. UPDATED INTELLIGENCE MISSION ANALYSIS
5

- 6 a. Weather analysis
7 b. Terrain analysis
8 c. Enemy situation & COAs
9

10
11 2. INTELLIGENCE STAFF ESTIMATE (may be part of combined staff estimate)
12

- 13 a. Assumptions used in planning
14 b. Results of staff estimate
15 c. Advantages and disadvantages (include risk) of each course of action
16 (with decision matrix or table showing course of action comparison)
17 d. Recommended course of action
18
19
20

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

INTELLIGENCE CONFIRMATION BRIEFING FORMAT

1. INTELLIGENCE ORIENTATION OF THE OPERATING AREA

- Weather
- Hydrography
- Topography
- Population
- Political Climate
- Points Of Entry (HLZs, airfields, ports, etc.) – Location, Description, etc.

2. ENEMY SITUATION

- Size
- Activity
- Identified Units (Location, Weapons, Equip, Uniform)
- Capabilities/Limitations
- Enemy COAs
 - Most Likely
 - Most Dangerous To Us
 - Most Advantageous To Us
- Expectations Upon Friendly Actions
- Reaction Force (Location, Weapons, Equip Uniform, Mobility)
- Special Equipment
- Identifications
- Intelligence and other Detection Capabilities
- Air Threats
 - Fixed Wing
 - Helicopter
 - Surface To Air
 - SAM
 - AAA
 - Radar Capabilities

3. SURVIVAL, EVASION, RECOVERY, ESCAPE (SERE) PLAN OF ACTION

- Recovery Sites
- Safe Areas
- Communications (Primary/Alternate)
- No Comms Plan (Night Far & Near; Day Far & Near)
- Extract Times (Primary/Alternate)

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 4. CHALLENGES AND PASSWORDS
- 2
- 3 5. INTELLIGENCE COLLECTION, REPORTING AND DISSEMINATION
- 4 REQUIREMENTS ON THE OBJECTIVE
- 5
- 6
- 7
- 8
- 9

Appendix E

**Guide to Preparing and Conducting
Intelligence Presentations**

This appendix provides a format to guide intelligence personnel, step by step, through the research, preparation and delivery of intelligence presentations and briefs.

BASIC PROCESS

I. Research and Preparation

Analyze your mission	Step	A
Consider your audience	Step	B
Identify objective and focus the brief	Step	C
Obtain and research intelligence and other info	Step	D
Determine the level of classification	Step	E
Establish a time line	Step	F
Conduct research	Step	G
Prepare an outline	Step	H
Plan for use of graphical and other visual aids	Step	I

II. Rehearsal

Create working papers and graphics	Step	J
Approximate memorization	Step	K
Reduce your material	Step	L
Practice sessions with a designated listener	Step	M

III. Delivery

The Location	Step	N
Body language	Step	O
Minimizing nervousness	Step	P

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

I. Research and Preparation

STEP A Analyze your mission.

Defining parameters or "boxing-in" the mission.

You must determine the scope and intent of the intelligence brief. There are four primary factors to consider: the audience and the occasion, the purpose of the brief, identifying relevant topics, and selecting a method of presentation.

STEP B Consider your audience.

1. Gauging the audience.

Analyzing your audience is one of the first and most crucial aspects in preparing an effective brief. Present problems and draw conclusions that will be easily understood by all. In other forums gauging the audience will not be as easy. Do not assume the level of detail/complexity your audience is capable of retaining. Ask questions, gauge their body language (i.e. rolling eyes, snoring, chuckles after each acronym, etc.) and most importantly prepare during the research phase. Questions to ask about your audience include:

1. How much do they know about the subject?
2. Does each individual in the audience know as much as everybody else? If not, who are the principal targets or decision makers?
3. Are they interested in the subject?
4. Are there reasons why they should be interested?
5. Do they have biases about the subject?

2. Playing the Audience.

Just as considering your audience is important before the brief, reacting to the attitude of your audience is important during the delivery. There are several techniques that are good rules of safety to follow:

- Avoid behaving in a conceited or antagonistic manner.
- Demonstrate a genuine concern for your listeners and exhibit a friendly attitude to relax yourself and your audience.
- Emphasize similarities between your listeners and you.
- Be honest and straight forward. Don't attempt to talk to a level or use words beyond your capability.
- Are there taboo subjects, phrases or words that will offend your audience?
- Establish with the audience a connection between your topic and their needs.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

STEP C Identify Objective and Focus the Brief.

Ensure it is appropriate to the audience planning and decisionmaking needs. Keep its scope focused on the supported PIRs, IRs, or other intelligence needs.

Objectives. When you begin to do your research and prepare your material, determine your primary objectives:

- Weather, environment and threat orientation?
- Friendly intelligence, CI and reconnaissance capabilities and limitations?
- COAs wargaming?
- Answers to previously stated PIRs, IRs and RFIs?
- Future or immediate planning and decisionmaking?

STEP D Obtain and research intelligence and other information.

The first step in researching an intelligence brief is an inventory of all the personal knowledge you have on the subject, followed by checking with personnel and intelligence already on hand. You will also want to check with external intelligence and other sources, such as NGOs and academics.

STEP E Determine the level of classification.

During tactical operations most intelligence briefs will be given at the SECRET level. However, if your target audience and facility supports SCI briefs, then consider the advantages and disadvantages of giving an SCI brief. Also, if allied, coalition partners, or other non-U.S. personnel will be in the audience, determine how this will affect the brief's content and classification.

STEP F Establish a time-line.

Establishing a time-line. Establishing a time-line from preparation through delivery is essential. Clearly delineate a research cut-off time. Also, plan for rehearsal time.

- Schedule a location for preparation.
- Ensure all necessary CIS support and accesses.
- Prepare a realistic time-line.
- Stick to the schedule you've created.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

STEP G Conduct research.

Research entails much more than simply reading material on your subject. You must evaluate, analyze, assess and reduce available intelligence and other information, organize it, and eventually verbalize it. To establish focus and ensure the brief supports the intelligence mission and tasks, you must:

- Isolate and prioritize intelligence questions.
- Turn your research needs into precise questions.
- Determine what kind of answers you need.
- Prepare a work file.
- Take notes, maintain them logically.
- Ensure pertinent intelligence collection and production leaders are aware of your task and needs to ensure that relevant new information and intelligence is brought to your attention as soon as it is available.
- Segment the material.

The last step, segmenting your material, involves preparing an outline. The outline should be made up of three main parts: the **Introduction**, **Body** and **Conclusion**. The outline should follow these basic principles:

- (1) Start by clearly identifying the PIRs, IRs, RFIs or other intelligence tasks.
- (2) List the major issues to be covered.
- (3) Bulletize sub-issues.
- (4) Conclude by restating the pertinent PIRs, IRs and RFIs, and then provide clear, relevant and tailored intelligence conclusions.

STEP H Prepare an outline.

In preparing an outline of your material, the simpler the better. A sample is provided.

1. PIR, IR, RFI or other Intelligence Task

2. Main Idea

- A. Supporting idea
- B. Supporting idea
- C. Supporting idea

3. Main Idea

- A. Supporting idea
- B. Supporting idea

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

4. Main Idea

A. Supporting idea

B. Supporting idea

C. Supporting idea

5. Conclusions

A. Supporting idea

B. Supporting idea

C. Supporting idea

6. Questions/New IRs

Storyboarding is another means of helping you visualize your flow. It can be done with a white board, butcher block paper or large note cards, and simply involves listing your main topics/ideas on top and all pertinent material pertaining to each point below. Step back, avoid concentrating on the material, and consider the flow. Does one point logically lead to the next? Can they be rearranged according to a strategy or purpose? This method will help you work on your transitions as you move from point to point, issue to issue. Whatever format you choose, you must be able to visualize the whole of your presentation at a glance. By doing so it will flow more naturally and you will not be intimidated by the quantity of information you are about to relay. Two tools you can use to format the brief's introduction and body are the acronyms INTROSH and PREP.

INTROSH (Interest/Need/Title/Revision/Objectives/Scope/Handouts) is also a useful tool in developing an introduction.

Interest - Build the audience's interest.

Need – Immediately relate to his/their intelligence needs.

Title - State the title, i.e, the PIR, IR, RFI or other supported intelligence task.

Revision - List or identify if there are any revisions.

Objectives - State the objectives of your brief.

Scope - List the scope of your brief.

Handouts/Notes - Are there any? When should you distribute them?

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

PREP (Point/Reason/Example/Point) can be a useful tool in developing the body of the brief.

Point - State the intelligence as it directly relates to the specific PIR, IR, RFI or other intelligence questions.

Reason – Immediately relate to current situation and planning and decisionmaking.

Example - Illustrate the intelligence with an appropriate example or reference to current or near-term tactical activities.

Point - Restate the main intelligence that the audience must understand.

STEP I Plan for use of visual aids.

1. The use of graphics and other visual aids.

Graphics and other visual aids are extremely important and, if used properly, enable your audience to remember what you've said and apply it to their needs. Graphics and visuals should conform to one or more of the following:

- Show how things look (as in photos).
- Show how things work (as in diagrams or models).
- Show how things relate to each other (e.g., threat force dispositions)
- Show important intelligence such as key words or key numbers.

2. Designing your graphics and other visual aids.

When designing graphics and other visuals there are 13 key issues to keep in mind.

- (1) Use simple terms, relationships, fonts, and graphics.
- (2) If a visual doesn't explain something better than words, it shouldn't be used.
- (3) A visual should never exceed 25 characters across (counting spaces).
- (4) It should have a minimum number of lines (no more than eight as a rule of thumb).
- (5) Only highlights should be shown.
- (6) A complete sentence should never be used. Only key words or phrases.
- (7) Cover only one idea per visual; don't dwell on it for more than a couple of minutes.
- (8) On graphs, use a minimum number of curves (try not to exceed three).
- (9) Use a minimum number of grid lines.
- (10) Eliminate supplementary notes.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- (11) Omit subtitles.
- (12) Never use vertical printing.
- (13) A visual for a brief should contain far less information than an illustration for a report or handout.

II. Rehearsal

Rehearsal is essential for many reasons, the most important of which are:

- 1. To gain enough familiarity and confidence that the right words come out effortlessly and naturally.
- 2. To allow easy use of graphics and other visual aids.
- 3. To look and feel more comfortable.
- 4. To stay focused on the intelligence objective and finish on time.
- 5. To make it easier to answer and anticipate questions.
- 6. Rehearsal may expose some gaps in your information, intelligence, or flaws in your logic.

STEP J Create working notes.

There are several techniques to organizing working notes and materials.

Time - Sequential organization is most appropriate for "how to" briefs, taking the audience through the logical steps.

Space - A top to bottom approach. Best suited to technical classes.

Cause/Effect - One of two strategies can be used. The first is a listing of certain conditions and contend that these will produce a given result or effect. The second strategy is the inverse of the first -- start with an effect and follow it up with the causes and conditions that drive it.

Problem/Solution - Extremely effective when providing recommendations to problems. You must be able to demonstrate that your solutions and recommendations are practical, realistic and desirable. This is best used when conducting a decision brief.

Pro/Con - Another effective strategy for decision briefs is the Pro/Con technique. The briefer impartially itemizes the advantages and disadvantages of a certain course of action or issue. The order in which you present the pro's and con's depends on many factors, but it is usually best to finish with the stronger portion or position.

Topical - A topical division of the main points of a talk involves determining categories of the subject.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

STEP K Approximate memorization.

A simple and effective method for memorizing your material is approximate memorization. Approximate, in that only a portion of the intelligence and other information needs to be committed to memory. If the main points covered and the material are well researched, the examples, related quotes, sub-issues, etc. will come naturally. This also allows flexibility for the briefer. If approximate memorization is used and the audience seems responsive only to certain elements, then the briefer can cull the information, expand on portions of it and avoid others.

Danger of verbatim memorization

By memorizing word by word instead of point by point, the material planned will certainly be the material covered. The danger in this is that the speaker becomes detached from the audience. In effect, it is a canned recital and often appears that way to the audience. Another problem with memorizing material word by word is "brief mental lapses". If even a single word is forgotten in a memorized speech, it may disrupt the briefer's thought process and briefing delivery.

STEP L Reduce your material.

The "half rule" is a tool that can help you in creating an effective brief. Simply put, the half rule is culling down your material by half before you begin your final rehearsals. For a 15 minute presentation, prepare 1/2 hours worth of material and reduce it to the most essential, effective issues. Having an impartial and honest opinion from someone while you rehearse will assist you in determining which points are unnecessary. Avoid slanted reasoning and irrational appeals. Slanted reasoning could be:

- Hasty/Rash generalizations.
- Faulty dilemmas and analogies.
- Stacked or unsupportable evidence.

Irrational appeals depend upon blind transfer of feelings from one thing to another without logical thought. This area could include:

- Name calling - putting people or things in a bad light by using uncomplimentary terms.
- Glittering compliments, praise and generalities.
- Appeals for the audience to get on the band wagon.
- The superior approach, "browbeating" or intimidating the audience with superior experience, information or qualities.
- The "plain folks" approach is based not in reasoning and logic but emotion. An example could be "Hey, I'm just learning too. I'm just here to get through this".

(See MCWP 2-12, chapter 3, for other analytical challenges and dangers.)

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

STEP M Run through with someone impartial.

Practice your brief with another intelligence Marine equally or more knowledgeable with the situation and intelligence questions. The more blunt and tactless your practice audience, the better your presentation will become.

III. Delivery

STEP N The Location.

Classroom Preparation

As well as preparing briefing material, the briefer has the responsibility for preparing the briefing location. He must ensure that the location is conducive to learning, that the furniture is arranged appropriately, and that the computer and audiovisual aids are all serviceable and properly set up. The briefer should try to control the physical environment so that it is conducive to learning. The following factors are important:

1. Lighting. Lighting should be adequate. If the audience is expected to read or write, then lighting must be bright. Ideally, lighting should be controllable from a single point accessible to the briefer.

2. Ventilation. Inadequate ventilation will cause the environment to become heavy causing lapses in concentration or dozing.

3. Distractions. The audience can be distracted by visual aids which are not immediately relevant. Accordingly, visual aids should be removed from sight when not in use. Posters, diagrams, etc., should be confined from visibility until needed during the brief.

4. Acoustics. A room with poor acoustics is tiring to brief in and it is irritating to the audience.

5. Seating. Comfortable seating is desirable in that it reduces lapses in the audience's concentration. A suitable writing surface is desirable to aid in note-taking. Seating layout is really a question of method, room size and shape, and type of activity. The most important criterion is that the briefer should be able to see all of the audience from his main briefing area, and that the audience should be able to see and hear the briefer as well as all of the graphics and visual aids.

STEP O Body language and other physical factors.

One can usually tell a good presentation from a bad one even if you cannot hear it. A speaker who is "bombing" typically shows it with gestures, posture, eye contact etc. There are

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

a few guidelines to follow to ensure the visual factors of a brief are a success.

Appearance. An audience sees you before it listens to you. Your uniform, haircut, shave is consciously and subconsciously evaluated by the audience before you begin to speak. Always be aware of your appearance. Appearance is also affected by your attitude. A nervous, fidgety person will set off alarm bells in the minds of the audience that you are uncomfortable and therefore won't put on a first-rate presentation. Remain outwardly calm; make the butterflies fly in formation.

Body Movement. Effective body movement involves the audience in your brief. Use it to accentuate, clarify, punctuate, illustrate, and put you and your audience at ease.

Use of the Voice. A good voice has two important characteristics: intelligibility and variation. It is reasonably pleasant, it is easily understood and it expresses differences in meaning.

- **Intelligibility** of your speech is affected by your articulation, pronunciation, vocalization and choice of words. Speak carefully, not slowly, intentionally avoiding poor grammar and stock expressions such as "OK," "like," "you know," "all right," and the like.

- **Variety** is the conscious avoidance of monotone delivery. 100 to 180 words per minute is the norm, but you should vary delivery tempo or pitch to stress points.

STEP P Minimizing nervousness.

Nervousness can have a positive as well as negative impact on a brief. Nerves or adrenaline will heighten your sense of awareness and mental acuity. Nerves can also cause you to fold in front of an audience, with many in the audience becoming as anxious and uncomfortable as the briefer.

Tips for the Terminally Nervous:

- You are not alone. Other intelligence professionals will be present to help.
- Be well prepared.
- Concentrate on what you have to say.
- Enthusiasm is the key.
- Hold good thoughts toward your audience and think of them as individuals.
- Develop a pre-brief routine to help you relax.
- Prep your body. Stretch your muscles, crack your knuckles, control your breathing.
- Visualize a successful performance. As you do your final mental run through, picture a

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

1 responsive audience with you out in front giving a confident, successful brief.
2

Appendix F

Intelligence Reports Formats

This appendix provides the formats for the following common types of all-source intelligence reports: Intelligence Summary (INTSUM), Intelligence Report (INTREP), Mission Report (MISREP), BDA Report, SALUTE Report, and Response to Request for Information (RRFI).

Section I. Intelligence Summary (INTSUM) Report Format

The INTSUM provides a summary of the reporting unit's intelligence situation covering a specified period of time. It is used to report threat activities, changes to threat capabilities, and the results of further collections, analysis and production to higher, adjacent, and subordinate forces. It is designed to update the current intelligence estimate and provide a continual intelligence assessment of threat actions and estimated capabilities and courses of action.

Guidance regarding the periodicity and deadline for submission of INTSUMs generally begins at the theater J2 level. Theater TTP and the specific OPLAN/OPORDER will designate INTSUM reporting requirements for subordinate JTFs or Service/functional components. Based on those requirements, the MAGTF G/S-2 will establish INTSUM reporting requirements for their major subordinate commands/elements (at the MEF CE level, this is the responsibility of the intelligence support coordinator). These requirements generally will be published as part of their OPLAN/OPORDER. The deadlines established are to allow the intelligence battalion's Production and Analysis (P&A) Cell sufficient time to incorporate subordinate INTSUMs into their own or other intelligence products. The G/S-2s of MAGTF major subordinate commands/elements will likewise determine INTSUM requirements for their headquarters and subordinate elements. Where possible, MEF TTP and SOPs, reflecting the TTP of anticipated theaters of operations, should establish standard INTSUM reporting requirements.

All units can produce INTSUMs, however, in practice they are normally generated at the MSC level or higher. The decision to produce INTSUMs at lower echelons must be balanced between the relatively small size of intelligence sections at regiment/group and battalion/squadron and the requirement for information and intelligence at higher command levels. A more abbreviated INTSUM format may be appropriate for lower tactical echelons, focused on significant threat actions and anticipated future actions.

At higher command levels, particularly JTFs and Unified Commands, a daily intelligence summary (DISUM) will usually be published every 24 hours. While INTSUMs, particularly at lower tactical echelons, provide a generally fine-grained but limited tactical perspective, the DISUM is broader in scope, potentially encompasses more aspects of a threat country's elements of national power, and focuses on operational-level intelligence analysis and estimates. MAGTF command elements tasked as JTF headquarters will generally be required to submit DISUMs to

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

the combatant command CINC. See the combatant command's TTP for the DISUM format. Although generally the same, formats may vary from theater to theater.

Below is provided a sample format for a written INTSUM that may be posted on a website. It is based generally on the intelligence estimate format. Like the estimate, the INTSUM should be tailored and focused to mission, the type of unit, and the information and intelligence needs of the commander. The format provided is representative of a format that would be used at the MAGTF or MSC level for conventional military operations. For military operations other than war (MOOTW), the below format generally will need to be modified to meet unique needs.

Note: For paragraphs not applicable to the reporting unit, the notation "NA" (not applicable) may be used, or the paragraph may be skipped (paragraph numbering should remain the same). If no significant information or intelligence is available for a particular paragraph, the notation "NSTR" (nothing significant to report) may be used. The annotation () reflects classification of that information line.

CLASSIFICATION/RELEASABILITY

INTSUM #: (Sequentially numbered such, as "DD-001-97")

DTG: DDHHMM(Time Zone) (Month) YY

INFO cutoff DTG

PERIOD: DDHHMM TO DDHHMM (Month) YY

I. () Highlights:

A. () Ground: Highlights of the current ground situation, usually divided by area or sector.

B. () Air: Highlights of the current air situation.

II. () Summary of Enemy Situation: (Each category should use the commander's related PIRs as the basis for the analysis and assessment.)

A. () Ground: Detailed analysis of the battlefield by area or sector with comments on projected activity in the next 12 hours.

B. () Air: Detailed analysis of the air and air defense situation with comments on projected activity in the next 12 hours.

C. () Naval: Detailed analysis of the naval situation with comments on projected activity in the next 12 hours.

D. () SSM/WMD: Detailed analysis of the SSM/WMD situation with comments on projected activity in the next 12 hours.

E. () Special Operations Forces (SOF): Detailed analysis of the SOF, force protection, and rear area security situation with comments on projected activity in the next 12 hours.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

F. () Other: May be used for detailed analysis of paramilitary, insurgent, terrorist, or other significant threat categories not discussed elsewhere. For MOOTW operations, separate paragraphs for each category of threat or significant power group may be created as necessary to either supplement or replace the above categories.

III. () MEF (or MSC) Assessment:

A. () Most Likely Course of Action:

B. () Most Dangerous Course of Action:

C. () Others (as necessary):

IV. () Enemy Movement During the Reporting Period: Major enemy units (to include at least two levels below that of the reporting command); include universal transverse mercator (UTM) coordinates of the new position.

V. () PIRs: The commander's current (previous and new) PIRs are listed here, each with a current assessment regarding the level of satisfaction of the intelligence requirement (i.e., partially satisfied, satisfied, not satisfied).

VI. () Intelligence Plans, Missions and Systems Status: Key intelligence collection, production, and dissemination plans updates; information on planned intelligence and reconnaissance missions; and intelligence systems status (generally only for those systems that are less than fully operational). The period covered by this paragraph will be per unit SOP or annex B to the operations order.

GRAPHIC INTSUM

In an effort to enhance the understanding of the INTSUM, and save time when disseminating, it is now common to graphically portray the INTSUM as a single or set of map overlays. With the proliferation of web-based automated information systems, it is increasingly common for INTSUMs to be "posted" in graphic and text formats, providing a wide range of MAGTF intelligence users the option to "pull" and use desired intelligence and products. By posting the graphics and supporting text products to a website (e.g., S-TDN, SCI-TDN, INTELINK or INTELINK-S), it is available to anyone with access to that site, to include G/S-3 personnel using systems such as TCO. Care must be exercised, however, to not place an over-reliance on electronically generated graphic INTSUMs. Graphics can require large bandwidth and processing power to be pulled over a web-based system, with possible degradation of the overall MAGTF tactical data network. Lower-level tactical units and allied nation forces may also not possess the means to access and use the information. This generally requires INTSUMs to be disseminated over multiple paths, both electronically and via hard copy (to sometimes include couriers), in both graphic and text form.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

The challenge with graphic INTSUMs, as with any graphic representation, is to convey essential intelligence and other information in a clear, concise, and easy to understand visual format. Because of the volume of detail to be presented, most graphic INTSUMs, particularly at higher commands, have evolved into multiple “slides” created with software such as Microsoft Power Point. There is no one approved format for graphic INTSUMs; they are established per unit SOP or the operations order (see annex B, *Intelligence*), tailored to the level of command, type of operation, and most importantly, the intelligence requirements of the commander. They do, however, generally contain the same elements. Listed below are some common elements of graphic INTSUMs. These should not be taken as absolutes, but instead as examples.

- **Weather Graphic(s)** - Composite graphics, based on satellite imaging, showing weather fronts, cloud coverage, high and low pressure areas, etc. for the area. May include forecast graphics for specified future periods.
- **5-Day Forecast** - Similar to television weather forecasts, showing forecast weather conditions (cloudy, partly cloudy, rainy, etc.), high and low temperatures, winds, normal temperatures based on climatology, and any other elements that may be of interest to the commander. Should also include light data for the same period.
- **Weather Impacts Graphic(s)** - Normally presented in “gumball” chart (green, yellow, red) format. Should include those forces, types of operations, or critical items of equipment that are essential to unit mission performance, both friendly and enemy.
- **PIRs** - Include current and new PIRs. May include assessment of level of satisfaction (not answered, partially answered, answered).
- **Activities and Assessments** - Consists of a graphical situation map, denoting locations of threat forces of interest and, if possible, graphically indicating status/combat effectiveness (color coding or other symbology). Depending on the level of command and information needs, separate graphics for categories of threat forces (ground, air, air defense) may be created to reduce clutter. Each graphic should:
 - Note significant threat activity over the reporting period, with text comment boxes tied to locations or an event numbering system with marginal text comments.
 - Provide an assessment(s) keyed to the commander’s PIRs.
 - Use supporting graphics to examine items in more detail, such as aircraft sortie analysis or the location and status of a particular category of force or equipment (i.e., heavy equipment transporter systems (HETs), specialized units, etc.)
- **Collection, Production, and Dissemination Plans; Status of Planned Missions** - Graphically presents locations of organic collection assets (reconnaissance teams, RadBn assets, UAV tracks, sensor strings, etc.) and/or provides a timeline showing daily projected availability windows and mission-tracks (as applicable) of non-organic supporting assets (AWACS, RC-135,

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

U2, etc.). Also identifies changes to previous production and dissemination plans and any new plans.

Outlook/Assessment- Provides overall assessment of estimated threat COA(s) (at a minimum, the threat's most likely/most dangerous COAs). It may be broken into estimate time periods, such as 24-48 hours, 48-96 hours, or whatever periods of time are applicable to the commands requirements to plan future actions. COAs should be graphically portrayed. In pre-hostilities or MOOTW, these graphics may be used to address anticipated political or societal actions/events that may impact on the force.

Section II. Intelligence Report (INTREP) Format

An intelligence report (INTREP) is a standardized report which is used to disseminate important intelligence without regard to a specific schedule. It can be prepared at any echelon by the first intelligence element acquiring the information and is disseminated as rapidly as possible to all units which may have need of the reported information. It may be prepared on any item of intelligence, regardless of source; generally, each report will concern only a single item.

An INTREP is generally required whenever an event occurs that is likely to result in a change in the friendly plan or when a change to the current or future analytical assessment is made. It is generally initiated when facts influencing threat capabilities have been observed, or when a change in threat capabilities has taken place. The commander's PIRs serve as the basis for determining what information warrants an INTREP. Whenever possible, the INTREP should include the originator's assessment of the significance of the intelligence, as well as an evaluation of the reliability and accuracy of the source. The format below provides an example of an INTREP format that would be posted on a website or forwarded via TDN or SIPRNET e-mail.

CLASSIFICATION/RELEASABILITY

INTREP#: DD-001-97 (Sequentially numbered by originating unit)

DTG: DDHHMM(Time Zone) (Month) YY

I. () Significant Event(s): A summation of the significant event(s) or developments that initiated the INTREP. Use either 5W (Who, What, Where, When, Why) or SALUTE (Situation, Activity, Location, Unit, Time, Equipment) format.

II. () Assessment: The effect of the current activity on threat capabilities or courses of action.

III. () Evaluation of Source: State the original source of the information and an evaluation of the accuracy and reliability of that source.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

Note: () Reflects classification of that information line.

Section III. Battle Damage Assessment (BDA) Report Format

The following is an example of a periodic summary battle damage assessment (BDA) report that may be used by MEF major subordinate commands' intelligence personnel to provide consolidated Phase I/Physical Damage Assessment BDA from their subordinates to the intelligence battalion's P&A Cell. The report is a compilation of BDA reporting from subordinate elements, as well as any additional BDA obtained at the MSC level during the designated time period. The aviation combat element would normally be responsible for providing BDA on any air tasking order (ATO) related missions, while the ground combat element would focus on the results of engagements by their subordinate elements, to include the observed effects of close air support.

The target intelligence/BDA team, P&A Cell, intelligence battalion, is responsible for consolidating, deconflicting, and refining these reports, introducing any additional information and intelligence obtained from other sources, and preparing the overall Phase I BDA (or Physical Destruction Assessment) for the MEF commander. The P&A Cell would also be responsible for adjusting the MEF order of battle (OOB) databases to reflect combat losses and developing the overall combat strength assessment for each unit. The P&A Cell target intelligence/BDA team would also prepare Phase II/Combat Strength Assessments based on the consolidated reporting from subordinate, higher and adjacent commands. Formats for BDA reporting to the JTF, theater, and national level will be established in the theater intelligence TTP or as directed by the joint task force commander.

SAMPLE BDA REPORT FORMAT

SUBJECT: 6 HR BDA REPORT (SUBMIT TO Intelligence Battalion's TgtIntel/BDA Team, P&A Cell, AT SPECIFIED TIMES)

REPORTING UNIT:

REPORTING PERIOD (FROM/TO):

ENEMY UNIT OR FACILITY #1: (DOWN TO BDE NAME FOR MANEUVER, BN FOR FIRE SUPPORT, or as directed in unit SOP or OPORD. REPEAT THIS SECTION FOR EACH UNIT OR FACILITY).

UIC OR BE#: DHGKNxxxxx

DAMAGED/DESTROYED

LOC

TYPE

#DEST

#DMGD/EXTENT

1. ARMOR:
2. FIRE SUPPORT:
3. TRUCKS:
4. AIR DEFENSE:

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

5. C2 SYSTEMS
6. MOB/CNTRMOB: (Engineers assets, bridges, lines of communication, mines,
etc.)
7. CSS:

LOC WIA KIA

8. PERSONNEL:

REMARKS:

IF UNIT NAME IS UNKNOWN, INCLUDE TIME OF REPORT (TOR), UNDER HEADING "ENEMY
UNIT: UNKNOWN". DO NOT SUMMARIZE: LIST EACH REPORT. FOR EXAMPLE:

ENEMY UNIT: **UNKNOWN**

UIC: **UNKNOWN**

DAMAGED/DESTROYED: LIST ALL UNKNOWN UNIT BDA REPORTS BY TIME

	<u>TOR*</u>	<u>LOC</u>	<u>TYPE</u>	<u>#DEST</u>	<u>#DMGD/EXTENT</u>
1. ARMOR:					
2. FIRE SUPPORT:					
3. TRUCKS:					
4. AIR DEFENSE:					
5. C2 SYSTEMS					
6. MOB/CNTRMOB: (Engineers assets, bridges, LOC's, mines, etc)					
7. CSS:					

	<u>TOR*</u>	<u>LOC</u>	<u>WIA</u>	<u>KIA</u>	<u>EPW</u>
8. PERSONNEL:					

REMARKS: *TOR: TIME OF REPORT. (NOTE: REMARKS ARE A MEANS OF REPORTING
INFORMATION THAT DOES NOT FIT INTO THE TABLES DESCRIBED ABOVE. SPELL IT OUT
IN A REMARKS SECTION, FOR EACH UNIT IF NECESSARY, IF YOUR ASSESSMENT GOES
BEYOND "BEAN COUNTING".

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

Section IV. Mission Report (MISREP) Format

PRECEDENCE

FROM:

TO:

INFO:

CLASSIFICATION

SUBJ: MISREP NO. _____/_____/Z/MONTH/YEAR

REF: (a) As appropriate.

BODY

1. Air Task/Mission Number or Nickname. Reference the request number, FRAGO number, or directive causing initiation of the mission.
2. Location Identifier. Target number, line number, approved target designator/identifier, or coordinates of the target or sighting being reported.
3. Time of Target/Time of Sighting. Report at all times by date/time group, using GMT unless otherwise directed.
4. Results/Sighting Information. This item should contain the pilot/aircrew evaluation of expected results (e.g., percent destroyed, number and type destroyed, or percent of coverage) and concise narrative information on significant sightings (e.g., unusual or new enemy equipment or concentrations of enemy forces observed to include number, speed, and direction, if applicable).
5. Remarks. Includes information and intelligence not specifically mentioned in above items (e.g., enemy defenses encountered; weather data; hostile electronic attacks; etc.).

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Section V. SALUTE Report Format

1. PURPOSE. The SALUTE report is submitted by units/personnel to report enemy activity or other intelligence information.

2. INFORMATION

- a. Classification. As required.
- b. Periodicity. As required.
- c. Due by. On occurrence.
- d. Period Covered. As required.
- e. Reporting Units.
- f. Method of Transmission
 - (1) Primary. Secure voice radio transmission.
 - (2) Secondary. Electronic data transmission.
 - (3) Tertiary. Courier.
- g. Precedence. As required.

3. ACTION. Submit a SALUTE report upon observation of significant enemy activity.

4. COMPLETION INSTRUCTIONS:

Line Alpha: Unit reporting and location.

Line Bravo: Size. Number of troops and approximate size and type of unit.

Line Charlie: Activity. Observed activity of the enemy.

Line Delta: Location. Position of enemy using UTM grid references.

Line Echo: Unit. Identity of enemy unit or description of markings, uniforms, equipment.

Line Foxtrot: Time. Date-Time-Group (local) of sighting.

Line Golf: Equipment. Number and description of weapons or equipment.

Section VI. Response To Request For Intelligence (RRFI) Format

1. PURPOSE. The RRFI is used to answer a Request for Intelligence (RFI).

2. INFORMATION

- a. Classification. As required.
- b. Periodicity. As required.
- c. Due by. On occurrence.
- d. Period Covered. As required.
- e. Reporting Units.
- f. Method of Transmission
 - (4) Primary. Electronic data transmission.
 - (5) Secondary. Secure voice radio transmission.
 - (6) Tertiary. Courier.
- g. Precedence. As required.

3. ACTION

- a. Submit RRFI as soon as the intelligence information is available, but NLT the LTIOV.
- b. **COMPLETION INSTRUCTIONS:**
 - (1) Line Alpha: IR or RFI number followed by requester and requester serial number.
 - (2) Line Bravo: Free text answer to the RFI.

Appendix G

**Intelligence Communications and Information
Systems (CIS) Plan Appendix Format**

Purpose. Tab D (Intelligence CIS Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) should explain how intelligence CIS elements under the operational control (OPCON) or supporting the MAGTF will be used to support the operations plan. It should also provide guidance to subordinate commanders for the conduct of intelligence CIS dissemination operations and the support of intelligence elements and personnel identified to fulfill the intelligence requirements in support of this plan.

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

**Tab D to APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B
(INTELLIGENCE) TO MAGTF OPORD X ()**
Intelligence Communications and Information Systems (CIS) Plan (U)

() **REFERENCES:** Identify organic DoD, DIRNSA, NIMA, and other directives; combatant commander, JTF, JFMCC/JFLCC/JFACC or other higher authorities' operations orders, tactics, techniques, and procedures (TTP), and standard operating procedures (SOP) for intelligence CIS operations; formats; and any other relevant documents that pertain to anticipated intelligence operations.

1. () **SITUATION**

a. () **Define the Area of Operations (AO) and Area of Interest (AOI).** Describe the limits of the AO and AOI. Summarize pertinent weather, terrain, and other AO characteristics and conditions as they may influence the conduct of intelligence CIS operations.

b. () **Enemy.** Refer to Annex B (Intelligence) and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence CIS operations.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

c. () Assigned MAGTF Organic and Supporting Intelligence CIS Assets. Identify organic and supporting forces available to perform C2 or intelligence CIS functions.

d. () Assumptions. (Derived during the mission analysis step of the Marine Corps planning process.)

e. () Intelligence CIS Considerations. List key intelligence CIS and interoperability considerations which impact this OPLAN or OPORD.

(1) () Availability of national and commercial intelligence and multi-purpose CIS resources.

(2) () Intelligence C2 and dissemination support to and from JTF/Component Headquarters and other external commands and intelligence organizations.

(3) () Creation and manning of forward intelligence C2 and operations elements.

2. () **MISSION**. State concisely the intelligence CIS mission as it relates to the command's planned operations.

3. () **EXECUTION**

a. () Concept of Operations. Summarize pertinent command relationships, task-organization, main and supporting efforts, and the scope of MAGTF and supporting intelligence CIS operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to intelligence operations. Outline the purpose and concept of intelligence CIS operations, specified priorities, and summarize the means and agencies to be employed to support the operations and intelligence concepts of operations. Address the integration of JTF, other components, theater, national, and allied forces' intelligence operations and CIS support.

b. () CIS Tasks for Intelligence Units and Organizations, Subordinate Units, and Detachment Commanders/OICs.

(1) () Orders to Subordinate, Attached, and Supporting Units. Use separate subparagraphs to list detailed instructions for each unit conducting intelligence-related dissemination operations, including the originating headquarters, subordinate commands, and separate intelligence support units.

(a) () Marine Division(s)

(b) () Marine Aircraft Wing(s)

(c) () Force Service Support Group(s)

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

(d) () Commanding Officer, Intelligence Battalion/Intelligence Support
Coordinator

1 () OIC, Support Cell

2 () OIC, Production & Analysis Cell

3 () OIC, Surveillance and Reconnaissance Cell

4 () Intelligence Systems Officer

5 () Commanding Officer, CI/HUMINT Company

6 () Platoon Commander, Imagery Intelligence Platoon

7 () Platoon Commander, Topographic Platoon

8 () OIC, Joint STARS Common Ground Station

(e) () Commander, Marine Corps Imagery Support Unit (if tasked to support)

(f) () Commanding Officer, VMU Squadron

(g) () Commanding Officer, VMAQ Squadron

(h) () Commanding Officer, Radio Battalion

(i) () Commanding Officer, Force Reconnaissance Company

(j) () OIC, National Intelligence Support Team (if attached)

(2) () Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached, or supporting and from which intelligence CIS support is requested, including other components, JTF headquarters, allied or coalition forces, theater, and national operational and intelligence elements.

c. () Coordinating Instructions. Reference Appendix 16 (Intelligence Operations Plan), Annex K (CIS), Annex J (C2), and command and other pertinent forces' and organizations' intelligence and CI SOPs. Detail here or in supporting tabs key changes to unit SOPs. Additional topics to include or emphasize here are: requesting CIS support, timely reporting procedures for intelligence CIS problems, coordinating switchover to backup dissemination paths, intelligence operations, C2, and CIS hand over between command echelons, etc.

4. () **ADMINISTRATION AND LOGISTICS**

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

a. () Logistics. Reference Annex D (Logistics). Identify intelligence CIS logistics requirements and concerns, such as: unique combat service support requirements (batteries, unique replacement parts), procedures, and other guidance to support MAGTF intelligence units and operations; procedures for specialized technical logistics support necessary from external organizations; map distribution; requirements for courier runs; etc.

b. () Personnel. Identify personnel requirements and concerns that affect intelligence CIS operations and support (systems administrators, global sourcing requirements, etc.).

5. () **COMMAND AND CONTROL**

a. () Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence intelligence operations and CIS support.

b. () Information Management. Reference Annex U (Information Management), Annex C (Operations) and Appendix 16 (Intelligence Operations Plan). Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence databases, reports, etc.) that will influence MAGTF intelligence CIS, reporting, and other operations.

c. () Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (CIS). Provide any instructions necessary regarding CIS that will influence MAGTF intelligence dissemination operations. List intelligence CIS priorities (by operational phase, intelligence units, intelligence operations and C2 nodes, intelligence activities – whichever approach is most effective for the operation).

d. () Intelligence C2 Nodes and Facilities. Reference the unit's SOP and Appendix 16 (Intelligence Operations Plan). Provide any guidance and instructions necessary regarding establishment and operation of intelligence C2 nodes and facilities and CIS support and priorities to these, to include, at a minimum: G/S-2 elements within future plans, future operations, current operations, and force fires centers; IOC's Support Cell, SARC and P&A Cell; CI/HUMINT Company CP; reconnaissance operations center; OCAC; command element tactical or rear echelons; and intelligence liaison elements.

Tabs

A Intelligence CIS Architecture Diagrams (See Appendix I for examples.)

- Include an diagram for the overall, overarching intelligence CIS architecture.
- Include diagrams by intelligence discipline (IMINT, SIGINT, HUMINT, etc.) if possible and useful for the operation.
- Include blueprints and CIS wire diagrams for all intelligence C2 and operations nodes and facilities, as appropriate.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- 1 B Intelligence Information Management Flow Diagram(s) (See figure 4-1 for one example.)
2

Appendix H

MAGTF Intelligence Dissemination Planning Checklist

Introduction. This appendix identifies typical dissemination planning and execution actions of the MAGTF command element's G/S-2 and Intelligence Battalion staff during each phase of the Marine Corps Planning Process (MCPD).

MCPD STEP	Actions of MAGTF Staff	Actions of MAGTF G/S-2 and Intel Battalion Staff
MISSION ANALYSIS	<ul style="list-style-type: none"> ✓ Identify the higher headquarters' (HHQ)/supported headquarters' intent. ✓ Identify tasks. ✓ Determine the area of operations (AO) and area of interest (AOI). ✓ Review available assets and identify personnel and equipment resource shortfalls. ✓ Determine constraints and restraints. ✓ Determine recommended commander's critical information requirements (priority intelligence requirements, friendly force information requirements, essential elements of friendly information). ✓ Identify requests for information. ✓ Determine assumptions. ✓ Draft the mission statement. ✓ Present a mission analysis brief. ✓ Draft the warning order. ✓ Convene/alert red cell (if appropriate). ✓ Begin staff estimates. ✓ Refine the commander's intent. ✓ Develop the commander's planning guidance. 	<ul style="list-style-type: none"> ✓ Review HHQ and MAGTF standing intelligence plans (e.g., Annex B to an OPLAN), pertinent memoranda of understanding, etc. ✓ Determine, coordinate with G/S-6, and establish dissemination procedures and CIS support for immediate intelligence planning and dissemination activities. ✓ Activate intelligence dissemination requirements (IDR) management procedures, databases, etc. ✓ Assist with determination of the MAGTF AO and AOI. ✓ Determine specified, implied and essential intelligence dissemination tasks. ✓ Begin development of proposed intelligence dissemination concepts of operation; coordinate closely with collection and production planners and all supported intelligence officers and intel/CI/recon units; obtain G/S-2 approval. ✓ Identify organic/supporting intelligence dissemination elements & points of contact (POCs) in all subordinate units; determine operational status of each; determine personnel and equipment deficiencies (special attention to CIS resources and capabilities, data management, courier requirements, and distribution). ✓ Identify JTF/multinational intelligence dissemination CIS

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

interoperability issues; provide recommendations.

✓ Establish/review/update the MAGTF intelligence dissemination standard operating procedures (SOPs) and planning and direction tools; special attention to:

➤ Identify intel dissemination support requirements.

➤ Prepare intelligence dissemination planning matrices (e.g., intelligence reports matrix and the dissemination matrix).

➤ Identify external organizations' intelligence dissemination plans and assess against MAGTF's initial requirements; determine deficiencies; initiate augmentation requests (coordinate with the ISC and G-2 plans officer).

✓ Validate/update JTF intelligence dissemination tactics, techniques and procedures (TTP) and MAGTF intelligence dissemination SOPs (coordinate with HHQ and subordinate units).

✓ Determine, validate and prioritize IDRs; identify deficiencies; special attention to those needed for COA development.

✓ Begin development of intelligence dissemination and CIS plans and modification of intelligence reporting SOPs; issue guidance to intelligence dissemination elements (coordinate with P&A Cell and SARC OICs).

✓ Initiate coordination with the G/S-3 information management (IM) officer regarding COP/CTP concept of operations, reporting, and other IM activities.

✓ Disseminate initial intelligence and CI estimates to subordinate units. Coordinate with P&A Cell OIC and subordinate intelligence officers regarding timelines and procedures for updates.

✓ Coordinate with the ISC, IMO, P&A Cell OIC, IIP and Topo Plt commander identification and

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

initial dissemination of geospatial information and imagery support.

- ✓ Coordinate with the IMO, ISC, and G/S-4 initial map and charts distribution.
- ✓ Coordinate courier dissemination support with the G/S-1.
- ✓ Coordinate with P&A Cell OIC and subordinate units' intelligence officers access to MEF intelligence databases.
- ✓ Activate G/S-2/IOC homepages (JWICS, SIPRNET, SCI-TDN, and S-TDN).
- ✓ Validate database management procedures for all-source and all single-source intelligence databases (coordinate with JTF).
- ✓ Establish initial IDR priorities.
- ✓ Ensure subordinate units' intelligence dissemination POCs kept advised of actions & developments.

**COURSE OF ACTION
DEVELOPMENT**

<ul style="list-style-type: none"> ✓ Continue intelligence preparation of the battlespace (throughout all steps of the planning process). ✓ Array friendly forces. ✓ Assess relative combat power. ✓ Centers of gravity and critical vulnerabilities analysis. ✓ Brainstorm possibilities. ✓ Develop roughcut course(s) of action (COA). ✓ Commander's input. ✓ COA(s) refinement. ✓ COA(s) validation. ✓ COA(s) graphic and narrative development. ✓ Prepare and present COA(s) briefing. ✓ Commander selects/modifies COA(s). 	<ul style="list-style-type: none"> ✓ Assist the intelligence section and other IOC cells with COA development. ✓ Develop an intelligence dissemination concept of operations for each COA; begin preparation of Tabs C, D, and E to Appendix 16 to Annex B. ✓ Determine intelligence dissemination capabilities required for each COA. Establish priorities with G/S-2 approval. ✓ Submit to G/S-6 detailed, prioritized list of intelligence CIS requirements (G/S-2, IOC, and all organic and supporting intelligence, CI and reconnaissance units). ✓ Update IDR priorities. ✓ Ensure subordinate units' intelligence dissemination POCs kept advised of pertinent actions and developments.
---	---

WARGAMING

<ul style="list-style-type: none"> ✓ Conduct COA analysis wargaming. ✓ Refine staff estimates and estimates of supportability. ✓ Develop concepts based upon 	<ul style="list-style-type: none"> ✓ Complete intelligence dissemination estimates of supportability for each COA designated by the G/S-2 or ISC. ✓ Assist P&A Cell OIC with
---	--

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

warfighting functions (as required).

- ✓ Prepare COA analysis brief.

completing the intelligence estimate and the friendly intelligence estimate of supportability.

- ✓ In coordination with ISC, P&A Cell OIC, and G-2 plans and operations officer, disseminate and manage intelligence support to staff and subordinate units to support COA wargaming.

- ✓ Continue dissemination

management in accordance with current PIRs/IRs and other guidance.

- ✓ Continue to monitor intelligence operations development and update intelligence dissemination plans.

- ✓ Ensure subordinate units receive necessary intelligence dissemination planning information; verify understanding; identify/update subordinates current IDRs.

- ✓ Validate and update MAGTF intelligence dissemination information requirements.

- ✓ Ensure subordinate units' intelligence dissemination POCs kept advised of pertinent actions and developments.

**COURSE OF ACTION
COMPARISON AND
DECISION**

- ✓ Evaluation of each COA
- ✓ Comparison of COAs
- ✓ Commander's decision
- ✓ Issuance of warning order

- ✓ Assist G/S-2, ISC and G-2 plans officer with evaluation and comparison of each COA.

- ✓ Continue development of dissemination and CIS plans and intelligence reports management consistent with the selected COA.

- ✓ Supervise intelligence and intelligence operations information dissemination to subordinate, supporting and external intelligence officers and planners to support the selected COA.

- ✓ Update, validate & prioritize IDRs and CIS requirements for the selected COA; issue guidance as appropriate to subordinate elements.

- ✓ Identify, initiate and coordinate intelligence CIS changes to support current operations.

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

- ✓ Coordinate intelligence CIS and dissemination element task-organization needs associated with the selected COA.
- ✓ Continue coordination with the G/S-6 regarding intelligence CIS requirements; coordinate with G/S-1 as necessary for physical courioring of intelligence products to subordinate units; and the G/S-4 for distribution of maps and charts.
- ✓ Continue coordination with the G/S-4 regarding intelligence CIS supply and transportation requirements.
- ✓ Review actions associated with satisfying intelligence CIS and dissemination personnel and equipment deficiencies associated with the selected COA.
- ✓ Ensure subordinate units receive pertinent intelligence CIS and dissemination guidance; verify understanding; identify/update subordinates' current IDRs.
- ✓ Validate and update MAGTF IDRs.
- ✓ Ensure subordinate units' intelligence dissemination POCs kept advised of pertinent actions and developments.

**ORDERS
DEVELOPMENT**

- ✓ Commander's intent is refined.
- ✓ Concept of operations turned into an operations order or a fragmentary order.
- ✓ Staff estimates and other planning documents are updated and converted into operations order (OPORD) annexes and appendices.
- ✓ Commander approves OPORD.
- ✓ Complete development of dissemination and intelligence CIS plans and intelligence reporting management; ensure copies are provided to subordinate units and they understand.
- ✓ Assist G/S-6 as required with development of Annex K.
- ✓ Assist G/S-3 as required with development of Annex U.
- ✓ Update, validate & prioritize IDRs.
- ✓ Update and issue intelligence CIS and dissemination guidance as appropriate to subordinate elements.
- ✓ Ensure pertinent intelligence products are disseminated to all subordinate units.

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

- ✓ Identify, prioritize and coordinate intelligence CIS requirements and support for deployment phases.
- ✓ Complete actions associated with personnel & equipment augmentation, interoperability issues, multinational dissemination, etc.
- ✓ Complete intelligence CIS, transportation and supply actions.
- ✓ Update IDR priorities.
- ✓ Maintain coordination with appropriate external organizations.

TRANSITION

- | | |
|--|--|
| <ul style="list-style-type: none">✓ Transition brief✓ Drills✓ Plan refinements (as required) | <ul style="list-style-type: none">✓ Assist intelligence section and ISC with transition brief.✓ Modify intelligence CIS and dissemination plans as necessary.✓ Modify intelligence reporting distribution as necessary.✓ Monitor ongoing intelligence dissemination operations; update and issue orders as appropriate to intelligence elements.✓ Ensure all intel dissemination POCs in JTF, other components, and subordinate units fully understand plans and standing requirements; and ensure they have received necessary intel products.✓ Participate in drills, as appropriate.✓ Monitor situation; PIRs/IRs; and initiate IDR and CIS priorities and actions as appropriate.✓ Remain engaged in MAGTF future plans activities. |
|--|--|

MCWP 2-13
COORDINATING DRAFT

Appendix I

MAGTF Intelligence Communications and Information Systems Architectures

Section I

Notional MEF Intelligence CIS Architectures

Introduction. The graphics in Section I illustrate the intelligence systems communications connectivity and overall intelligence communications and information systems (CIS) architecture for the following:

- The Marine Expeditionary Force (MEF) main command post C2 nodes and combat intelligence center
- The Intelligence Battalion, its Intelligence Operations Center, and its key subordinate battalion elements
- The Marine Division main command post, Reconnaissance Battalion, and LAR Battalion
- The Marine Aircraft Wing headquarters air combat intelligence center
- The Force Service Support Group headquarters intelligence section and CSSD combat service support operations centers
- The MEU(SOC) amphibious task force intelligence center and select other C2 centers
- Various Marine intelligence, counterintelligence, and reconnaissance units

All information shown is notional – the actual CIS architecture used for any operation will be consistent with METT-T, commander’s guidance, concepts of operation, and other key factors.

Each graphic is followed by a supporting table. These tables reflect the direction of the communication path for the connection, the communication link designator, addressed in the last table, I-22, “Standard Communications Pathways and Connectivity,” and the internal message format that may be used. Table I-22 also contains the type of physical communication link used between systems, the data link layer protocol used, the network layer protocol used, the transport layer protocol used, and the type of message header used in the information exchange. Finally, table I-22 also lists the modem, switch or server, and cryptographic equipment normally used in that communication link or pathway.

MCWP 2-13
COORDINATING DRAFT

1 All figures and supporting tables are organized by the intelligence C2 or intelligence operations node, showing those intelligence
2 systems and communications systems typically employed within each. Again, all information shown is notional -- METT-T
3 factors as well as variations in unit SOPs will determine the specific intelligence systems and CIS architecture used for a particular
4 operation.

5
6 In addition to this information, please refer to the organization and responsibilities, the command and control, and the CIS chapters
7 and supporting appendices of the various intelligence series MCWPs for additional information on intelligence, CI and
8 reconnaissance CIS architectures.

MCWP 2-13
COORDINATING DRAFT

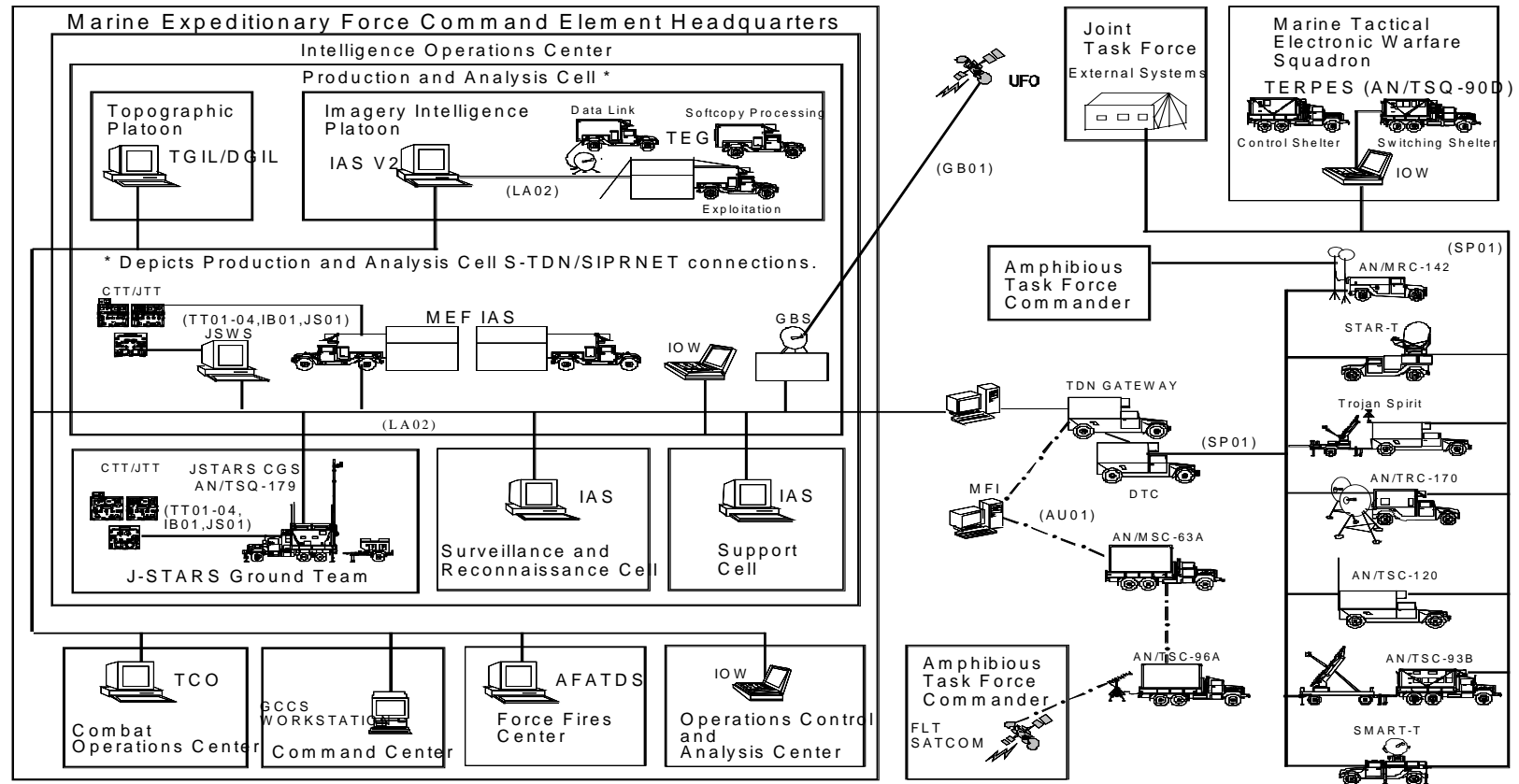


Figure I-1. MEF CE Combat Intelligence Center and Intelligence Battalion Intelligence IOC GENSER Systems Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS	JSWS	IOW	CTT-JTT	TGIL/DGIL	IAS V2	FLTSATCOM	AN/TRC-170 AN/TSC-120 TS II STAR-T AN/TSC-85-93
Intel Ops/C2 Node	Intel Bn P&A Cell	Intel Bn P&A Cell	Intel Bn P&A Cell	Intel Bn P&A Cell	TOPO PLT	IIP	ATF COMD & EXTERNAL SYSTEMS	EXTERNAL SYSTEMS
MEF CE P&AC IAS								
Comm Net							TCC to the AN/TSC-96A	
Direction	B	B	B	R	B	B	B	B
Comm Links	LA01	LA02	LA02	TT01-04, & IB01	LA02	LA01	AU01	SPO1
Internal Message Format	OTH-G, VMF	OTH-G, USMTF, VMF, NITF	VDX	Presently proprietary under IBS will be TADIL-J and VMF	OTH-G, USMTF, CADRG, GEOTI F, VPF & OTHERS	OTH-G, USMTF, NITF	OTH-G, USMTF	OTH-G, USMTF, VMF, NITF
Systems	IAS IOW	J-STARS CGS	IOW	GBS	IAS V2	TCO	GCCS	AFATDS
Intel Ops/C2 Node	VMAQ	Intel Bn J-STARS GRND TM	MEF CE & Radio Bn OCAC	Intel Bn P&A Cell	Intel Bn SARC	MEF CE COC	MEF CE CMD CTR	MEF CE FFC
Intel Bn P&A Cell MEF IAS								
Comm Net	AN/TRC-170 AN/TSC-120 TS II							
Direction	B	B	B	R	B	B	B	B
Comm Links	SPO1	LA02	LA02	CD01/LA02	LA02	LA02	LA02	LA02
Internal Message Format	OTH-G USMTF, VMF, NITF	OTH-G USMTF, NITF, VMF	VDX	MPEG-2, NITF (In SMTP or FTP), NTSC, DVB	OTH-G, VMF, NITF	OTH-G USMTF, NITF	OTH-G USMTF	OTH-G USMTF, VMF

Table I-1. MEF CE CIC and Intelligence Battalion IOC GENSER Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

1

Systems	CIHEP	TRSS
Intel Ops/C2 Node	CI/HUMINT Rep in SARC	Ground Sensor Platoon Rep in SARC
Intel Bn P&A Cell IAS		
Comm Net		
Direction	B	B
Comm Links	LA01	LA01
Internal Message Format	OTH-G, USMTF, NITF & OTHERS	OTH-G, SENREP (In USMTF)

2

3

4

5

Table I-1. MEF CE CIC and Intelligence Battalion IOC GENSER Systems and Communications Interface Requirements (cont.)

MCWP 2-13
COORDINATING DRAFT

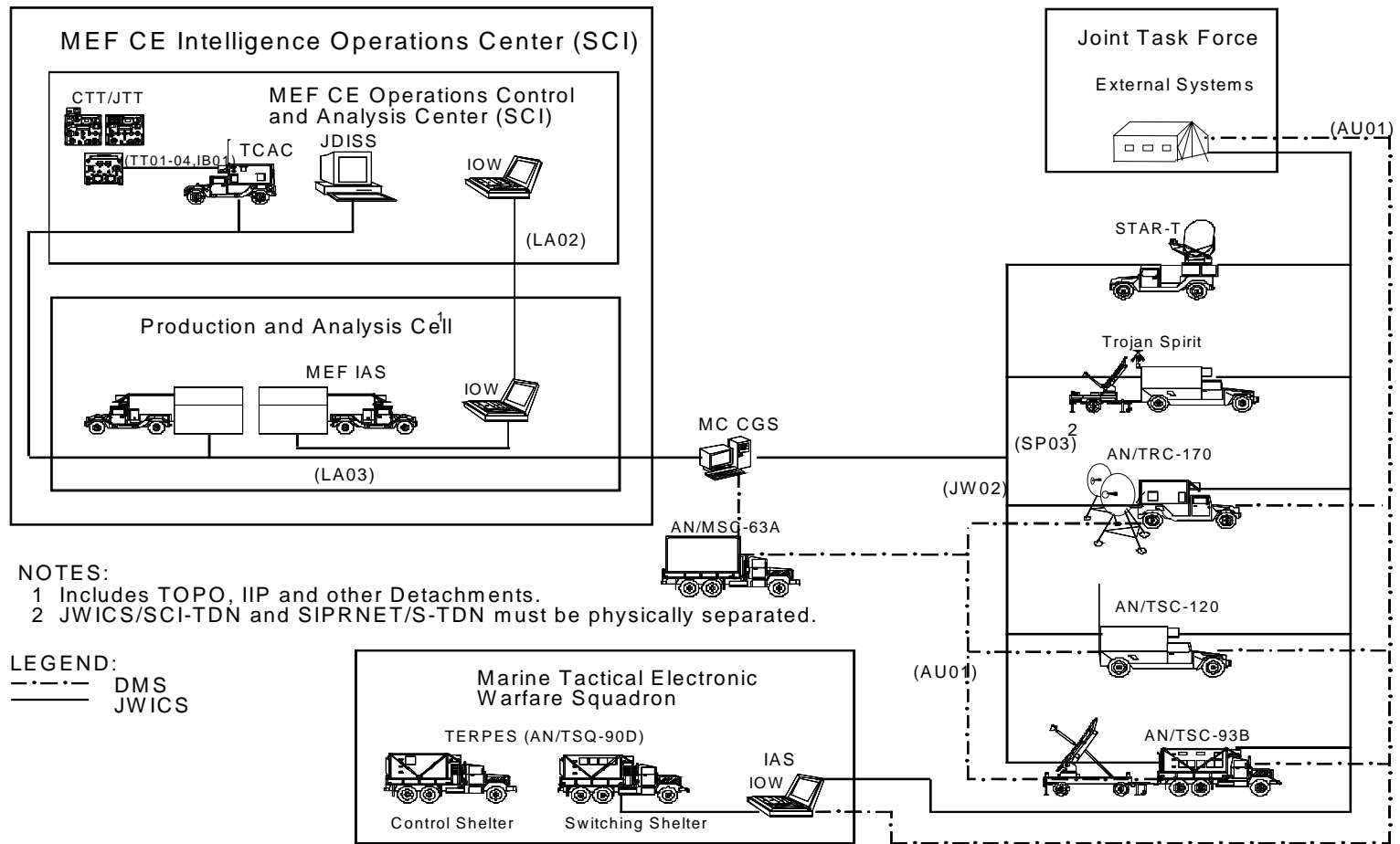


Figure I-2. MEF Command Element Combat Intelligence Center and Intelligence Battalion IOC – SCI Systems Architecture

MCWP 2-13
COORDINATING DRAFT

1

Systems	MEF IAS	TGIL/DGIL	IAS V2	JDISS	TCAC	TACINTEL	SSCC
Intel Ops/C2 Node	Intel Bn P&A Cell	TOPO PLT	IIP	Intel Bn P&A Cell	MEF CE & Radio Bn OCAC	ATF SSES	EXTERNAL SYSTEMS
MEF CE A&PC MEF IAS							
Comm Net						SSCC to the AN/TSC-96A	
Direction	B	B	B	B	B	B	B
Comm Links	LA01	LA02	LA01	LA02	LA02	AU01	AU01
Internal Message Format	OTH-G, VMF	OTH-G, USMTF, CADRG,GEOTI F,VPF & OTHERS	OTH-G, USMTF, NITF	OTH-G, USMTF, NITF	OTH-G, USMTF	OTH-G, USMTF,	OTH-G, USMTF,
Systems	AN/TRC-170 AN/TSC-120 TS II SMART-T AN/TSC-85-93	IAS IOW					
Intel Ops/C2 Node	EXTERNAL SYSTEMS	VMAQ					
Intel Bn P&A Cell MEF IAS							
Comm Net		AN/TRC-170 AN/TSC-120 TS II					
Direction	B	B					
Comm Links	JWOI	JWOI					
Internal Message Format	OTH-G, NITF, SMTF, VMF	OTH-G, USMTF, VMF, NITF					

2

3

4

5

6

Table I-2. MEF CE CIC and Intelligence Battalion IOC SCI Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

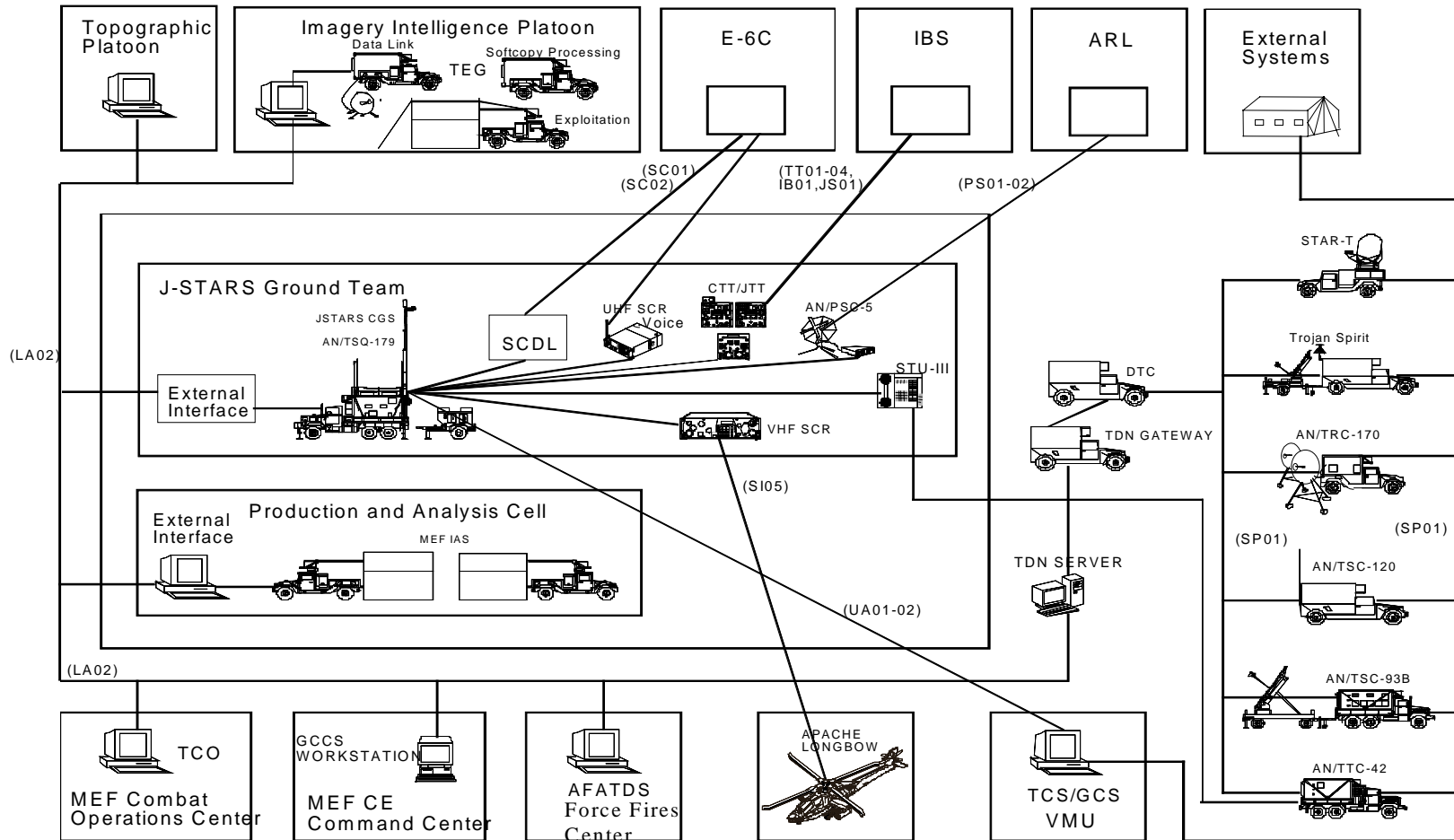


Figure I-3. Intelligence Bn IOC J-STARS CGS Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	TGIL/DGIL	IAS V2	JSTARS	JSTARS	JSTARS	CTT-JTT	AN/TRC-170 AN/TSC-120 TS II STAR-T AN/TSC-85-93	ARL
Intel Ops/C2 Node	TOPO PLT	IIP	E-8C	E-8C	E-8C	Intel Bn P&A Cell	EXTERNAL SYSTEMS	
MEF CE JSTARS GRND TM JSTARS CGS								
Comm Net								
Direction	B	B	R	B	B	R	B	B
Comm Links	LA02	LA01	SC02	SC01	AN/VRC-83	TT01-04, IB01	SPO1	PS01-02
Internal Message Format	OTH-G, USMTF, CADRG,GEO TIF,VPF & OTHERS	OTH-G, USMTF,NITF	SAR, MTI, FTI	C2	Voice	Presently proprietary under IBS will be TADIL-J and VMF	OTH-G, USMTF, VMF	NITF
Systems	MEF IAS	JSWS		TCO	GCCS	AFATDS	APACHE	TCS
Intel Ops/C2 Node	Intel Bn P&A Cell	Intel Bn P&A Cell		MEF CE COC	MEF CE CMD CTR	MEF CE FFC	Longbow	VMU
MEF CE JSTARS CGS GRND TM								
Comm Net								
Direction	B	B		B	B	B	B	B
Comm Links	LA02	LA02		LA02	LA02	LA02	SI05	UA01-02
Internal Message Format	OTH-G, USMTF, NITF	OTH-G, USMTF		OTH-G, USMTF; VMF	OTH-G, USMTF	OTH-G, USMTF; VMF	MTI Data	Video Telemetry

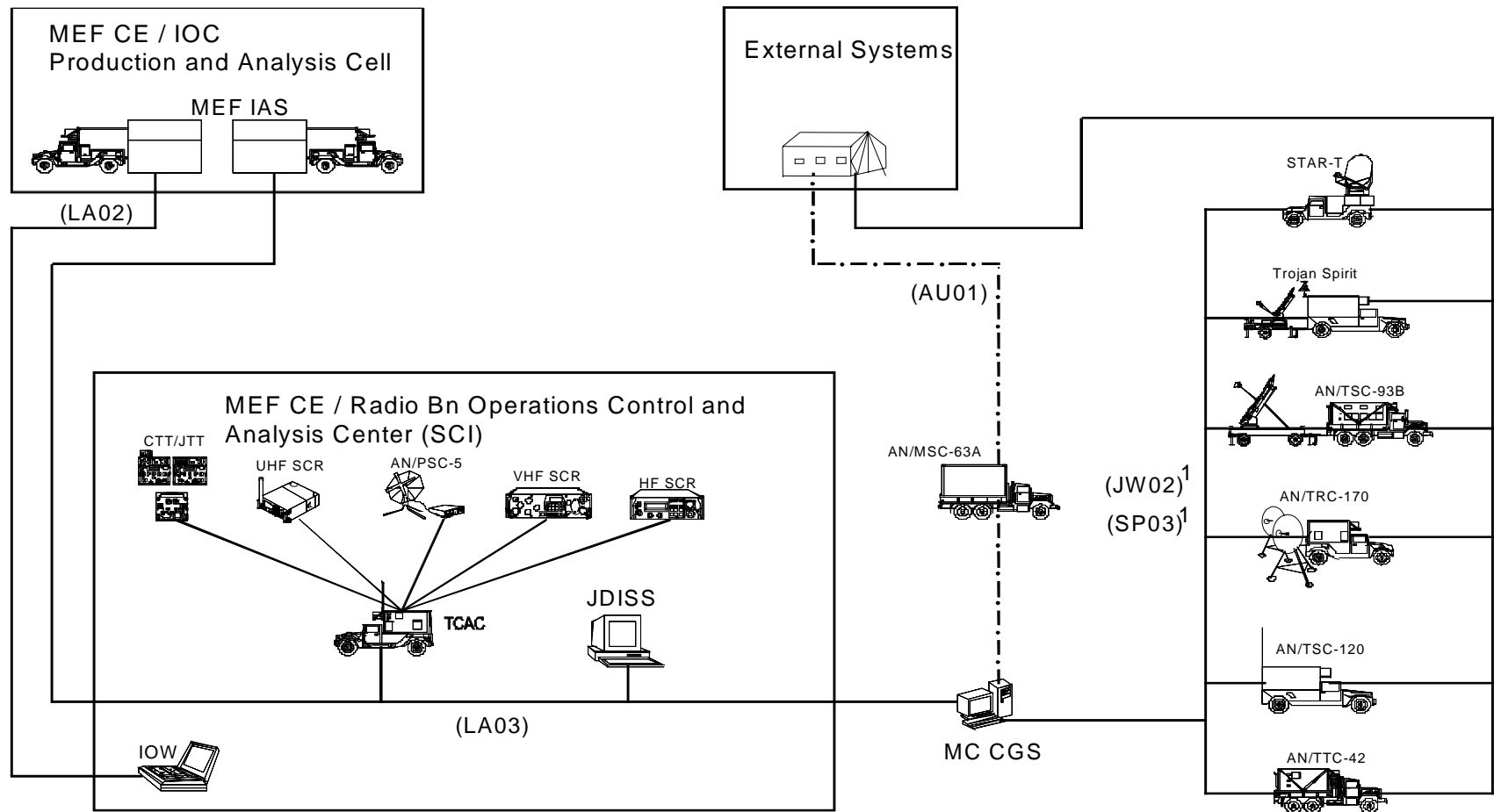
Table I-3. Intelligence Bn IOC J-STARS CGS Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

Systems	JSTARS CGS			
Intel Ops/C2 Node	Intel Bn JSTARS GRND TM			
Intel Bn JSTARS CGS GRND TM JSTARS CGS				
Comm Net				
Direction	B			
Comm Links	LA01			
Internal Message Format	Internal			

Table I-3. Intel Bn IOC J-STARS CGS Systems and Communications Interface Requirements (cont.)

MCWP 2-13
COORDINATING DRAFT



NOTES:

1. JWICS/SCI-TDN and SIPRNET/S-TDN must be kept physically separated.

LEGEND:

- DMS
- SIPRNET/S-TDN

Figure I-4. MEF CE and Radio Battalion OCAC Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	JDISS	CTT-JTT	AN/VRC-92A	AN/PSC-5	AN/GRC231A(V)P	AN/TRC-170 AN/TSC-120 TS II SMART-T AN/TSC-85-93	MEF IAS
Intel Ops/C2 Node	MEF CE & RadBn OCAC	MEF CE & RadBn OCAC	MEF CE & RadBn OCAC	MEF CE & RadBn OCAC	MEF CE & RadBn OCAC	EXTERNAL SYSTEMS	Intel Bn P&A Cell
TCAC							
Comm Net							
Direction	B	R	B	B	B	B	B
Comm Links	LA03	TT01-04, IB01	SI02	PS01-02	PR01	JWOI	LA02
Internal Message Format	OTH-G, USMTF	TADIL-J and VMF	USMTF, USSID, VMF	USMTF, USSID, VMF	USMTF, USSID, VMF	USSID, USMTF	USMTF VMF
Systems		IAS					
Intel Ops/C2 Node IOW MEF CE OCAC		MEF CE P&AC					
Comm Net							
Direction		B					
Comm Links		LA01					
Internal Message Format		VDX					

Table I-4. MEF CE and Radio Battalion OCAC Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

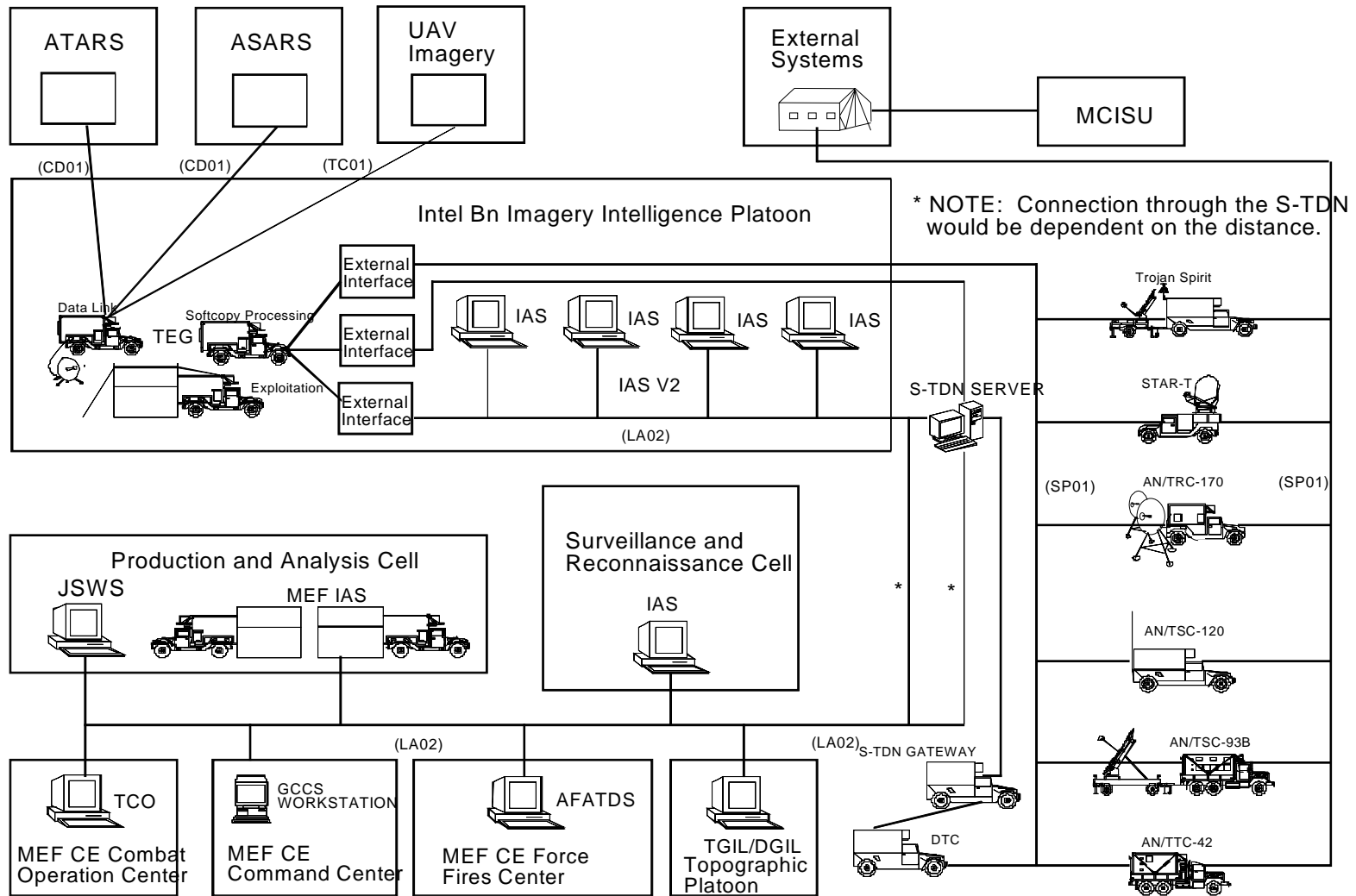


Figure I-5. Intelligence Bn Imagery Intelligence Platoon Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	TEG	ATARS	ASARS	UAV IMAGERY	TS II	AN/TRC-170 AN/TSC-120 TS II STAR-T AN/TSC-85-93	IAS V2
Intel Ops/C2 Node	IIP	F-18	U-2	VMU	MEF CE TECH CON	EXTERNAL SYSTEMS	IIP
IIP TEG							
Comm Net							
Direction	B	R	R	R	B	B	B
Comm Links	LA01	AT01	CD01	TC01	SP04	SP01	LA01
Internal Message Format	Internal	E/O,	SAR	NTSC, E/O	NITF., VIDEO	NITF.2, USMTF	OTH-G, VMF, USMTF
Systems	IAS V2	JSWS	MEF IAS	IAS V2	TCO	GCCS	AFATDS
Intel Ops/C2 Node IIP IAS V2	IIP	P&A Cell	P&A Cell	SARC	MEF CE COC	MEF CE CMD CTR	MEF CE FFC
Comm Net							
Direction	B	B	B	B	B	B	B
Comm Links	LA01	LA02	LA01	LA02	LA02	LA02	LA02
Internal Message Format	OTH-G, VMF, USMTF, NITF	OTH-G, USMTF, VMF, NITF	OTH-G, VMF, NITF	OTH-G, VMF, NITF	OTH-G USMTF	OTH-G USMTF	OTH-G USMTF, VMF

Table I-5. Intelligence Bn Imagery Intelligence Platoon Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

1

Systems	TGIL/DGIL
Intel Ops/C2 Node IIP IAS V2	TOPO PLT
Comm Net	
Direction	B
Comm Links	LA02
Internal Message Format	OTH-G, USMTF, CADRG, GEOTIF, VPF & OTHERS

2

3 Table I-5. Intelligence Bn Imagery Intelligence Platoon Systems and Communications Interface Requirements (cont.)

MCWP 2-13
COORDINATING DRAFT

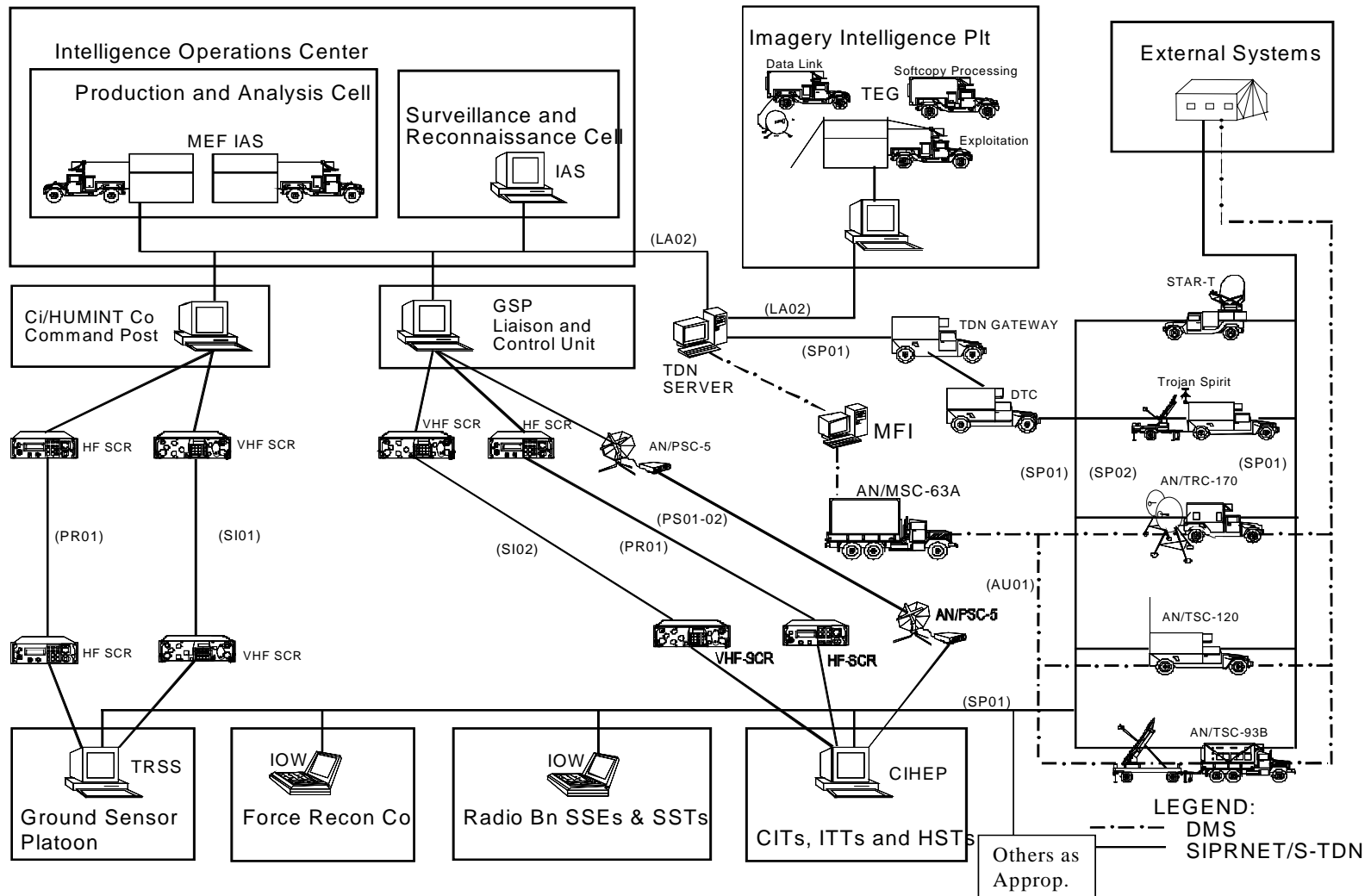


Figure I-6. Intelligence Bn IOC Surveillance and Reconnaissance Cell

MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS	IAS V2	AN/TRC-170 AN/TSC-120 TS II STAR-T AN/TSC-85-93	TCC			
Intel Ops/C2 Node	Intel Bn P&A Cell	IIP	EXTERNAL SYSTEMS	EXTERNAL SYSTEMS			
MEF CE SARC IAS							
Comm Net							
Direction	B	B	B	B			
Comm Links	LA02	LA02	SP01	AU01			
Internal Message Format	OTH-G, USMTF, NITF	OTH-G, USMTF, NITF	OTH-G, USMTF, VMF, NITF	JANAP 128 DOI-103			
IAS	TRSS	MANPACK SIDS	CIHEP	MANPACK SIDS	CIHEP	CIHEP	
INTEL BN SARC	SENSOR PLT	RECON	RECON	LA BN	LA BN	LA BN	
Comm Net							
Direction	Sensor Net						
Comm Links	R	R	R	R	R	R	
Internal Message Format	PR01 / SI04	SP01	SP01	SP01	SP01	SI01	
	SENREP (USMTF)	NITF Imagery	NITF Imagery & Tape	NITF Imagery	NITF Imagery & Tape	VMF	

Table I-6. Intelligence BN IOC SARC Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

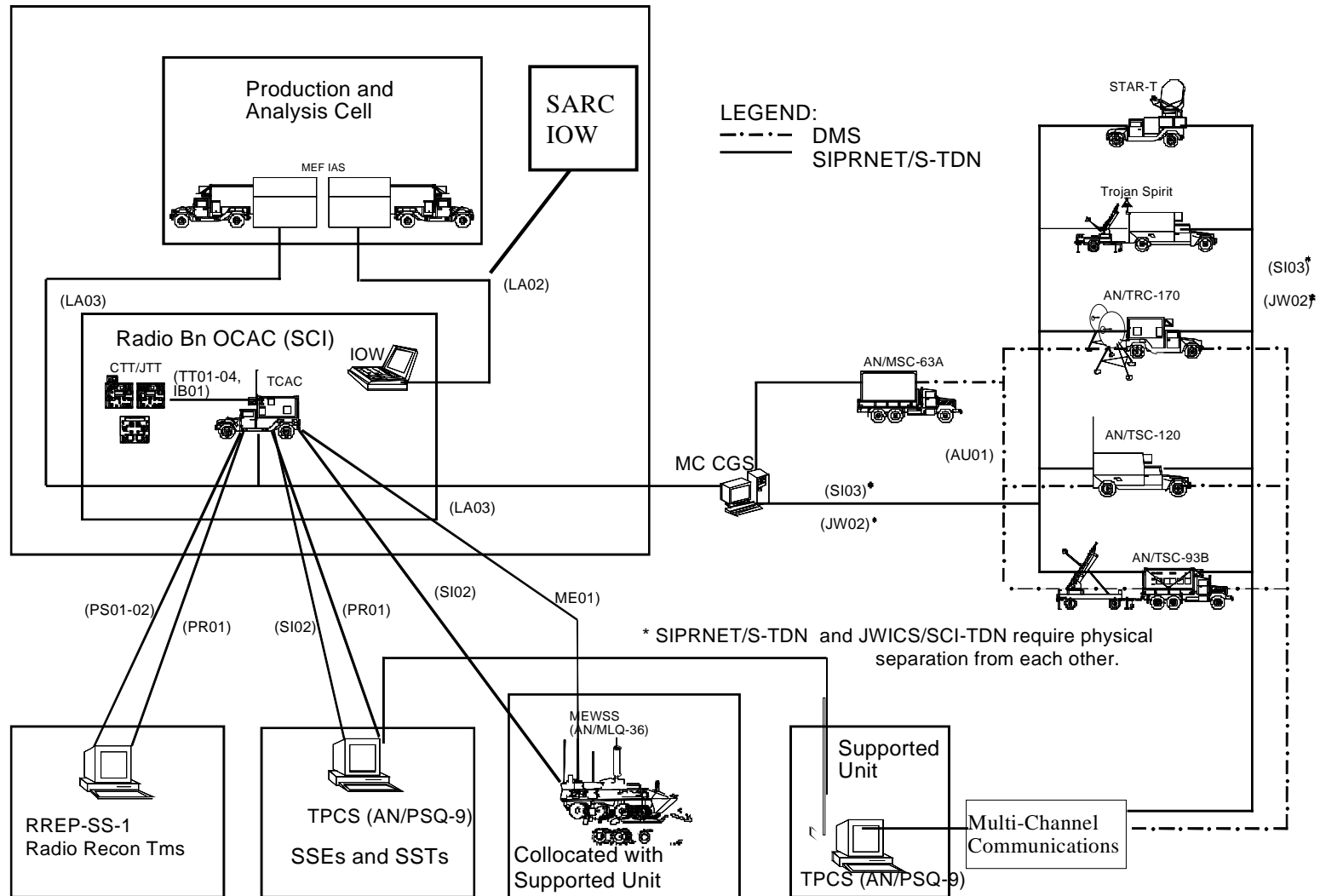


Figure I-7. Radio Battalion C2, Operations and Collection Systems Architecture

MCWP 2-13
COORDINATING DRAFT

1

Systems	IAS	AN/TRC-170 AN/TSC-120 TS II SMART-T AN/TSC-85-93	TPCS	RREP-SS-1	TPCS	RREP-SS-1	TPCS	TPCS
Intel Ops/C2 Node	Radio Bn OCAC	EXTERNAL SYSTEMS	RAD BN SSEs & SSTs	RRT	RAD BN SSEs & SSTs	RRT	RAD BN SSEs & SSTs	SUPPORTED ORG
TCAC OCAC								
Comm Net			Via AN/PSC-5	Via AN/PSC-5	Via AN/VRC-92A	Via AN/GRC231A (V)P	Via AN/GRC231A (V)P	Via SSCC
Direction	B	B	B	B	B	B	B	B
Comm Links	LA03	JWO2	PS01-02	PS01-02	SI02	PR01	PR01	AU01
Internal Message Format	USMTF, VMF	USSID, USMTF	USSID, VMF USMTF	USSID, VMF	USSID, VMF	USMTF USSID, VMF	USSID, VMF	USSID USMTF
System TCAC	MEWSS PIP	MEWSS PIP		IOW	MEF IAS			
Intel Ops/C2 Node OCAC	LAR Bn/Other	LAR Bn/Other		OCAC	Intel Bn P&A Cell			
Comm Net	Via AN/GRC231A (V)P	Via MECDL						
Direction	B	B		B	B			
Comm Links	PR01	ME01		LA02	LA02			
Internal Message Format	USMTF USSID, VMF	IEWCOMCAT DOI-103 USSID VMF		VDX	USMTF, VMF			

2

3

4

Table I-7. Radio Battalion C2, Operations & Collection Systems Interface and Communications Requirements

5

**MCWP 2-13
COORDINATING DRAFT**

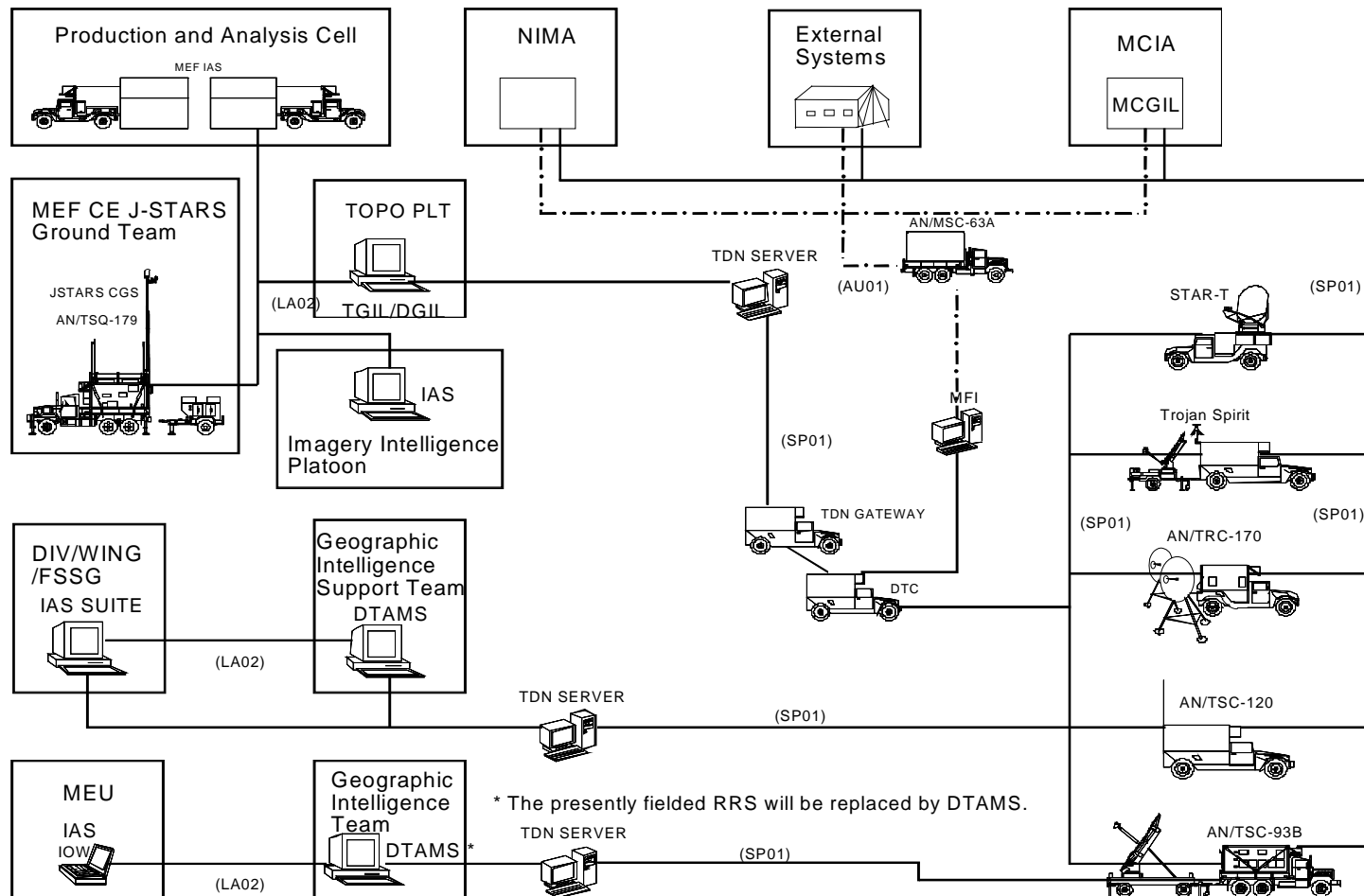


Figure I-8. Topographic Platoon, Intelligence Bn, Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	J-STARS LAN	MEF IAS	IAS	IPL	AN/TRC-170 AN/TSC-120 TS II STAR-T AN/TSC-85-93	MCGIL	TCC
Intel Ops/C2 Node	MEF J- STARS GRND TM	Intel Bn P&A Cell	MEF CE IIP	NIMA	EXTERNAL SYSTEMS	MCISU	EXTERNAL SYSTEMS
TOPO PLT TGIL/DGIL							
Comm Net							
Direction	B	B	B	B	B	B	B
Comm Links	LA02	LA02	LA02	SP01	SP01	SP01	AU01
Internal Message Format	OTH-G, USMTF, CADRG,GE OTIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEO TIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEO TIF,VPF & OTHERS	CADRG, VPF	OTH-G, USMTF, CADRG,GEOTIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEOTIF, VPF & OTHERS	USMTF
Systems	IAS V2	TGIL/DGIL	MCGIL	DMS	DTAMS	IOW (IAS)	
DTAMS GIST	DIV/WING/ FSSG	TOPO PLT	MCIA	NIMA	GIT	MEU	
Comm Net		Via Multi-channel	Via Multi-channel	TCC			
Direction	B	B	B	B	B	B	
Comm Links	LA02	SPO1	SPO1	AU01	LA02	LA02	
Internal Message Format	OTH-G, USMTF, CADRG,GE OTIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEO TIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEO TIF,VPF & OTHERS	OTH-G, USMTF	OTH-G, USMTF, CADRG,GEOTIF,VPF & OTHERS	OTH-G, USMTF, CADRG,GEOTIF, VPF & OTHERS	

Table I-8. Topographic Platoon Systems and Communications Interface Requirements

**MCWP 2-13
COORDINATING DRAFT**

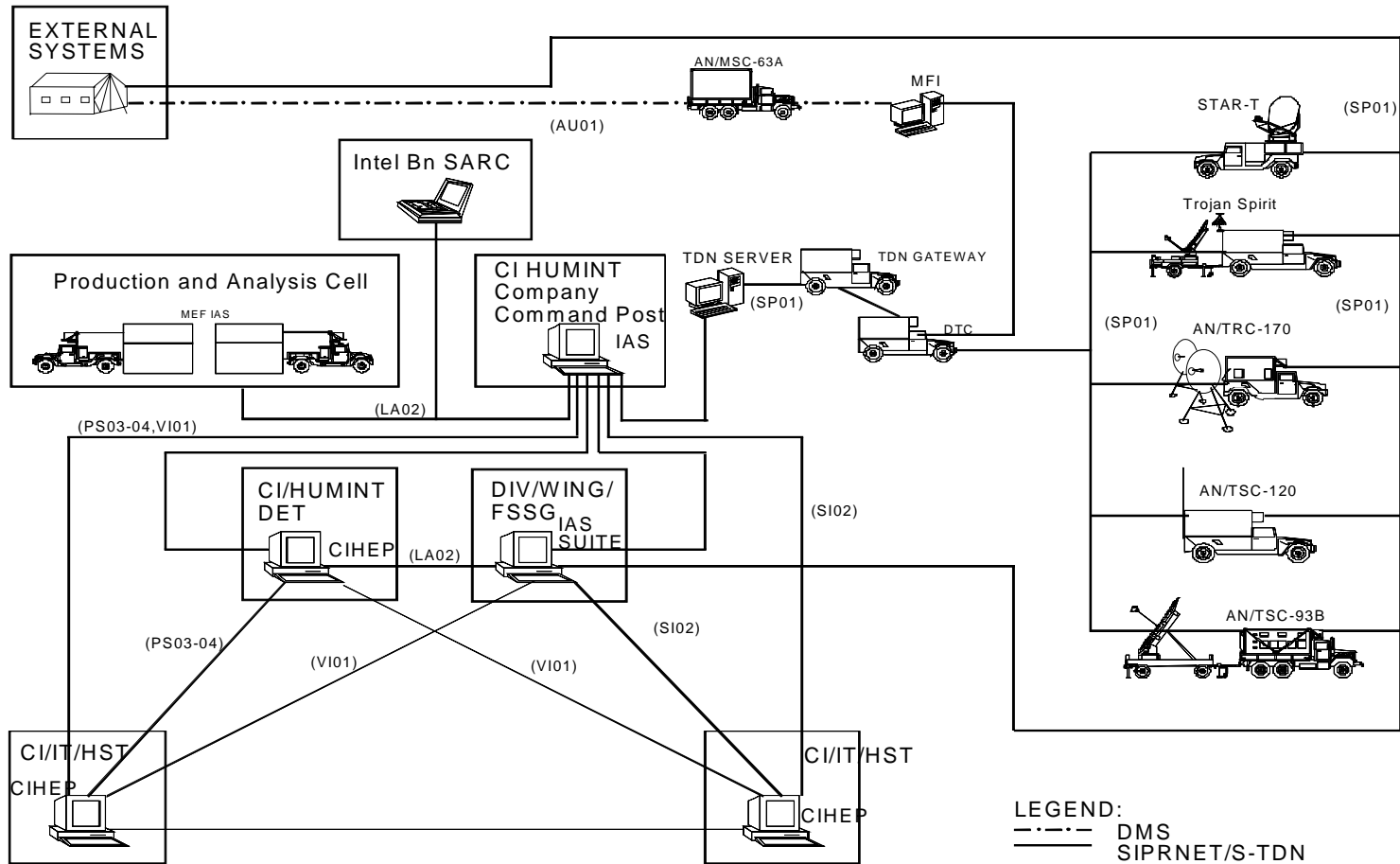


Figure I-9. CI/HUMINT Company, Intelligence Battalion, Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	CIT/TTT/HST	IAS SUITE
Intel Ops/C2 Node		DIV/WING/FSSG
CI/HUMINT Co Dets		
Comm Net		
Direction	R	B
Comm Links	VI01,PS03-04, PR01, SI02	LA02
Internal Message Format	IMAGERY, NITF, VMF	NITF

Table I-9. CI/HUMINT Company Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

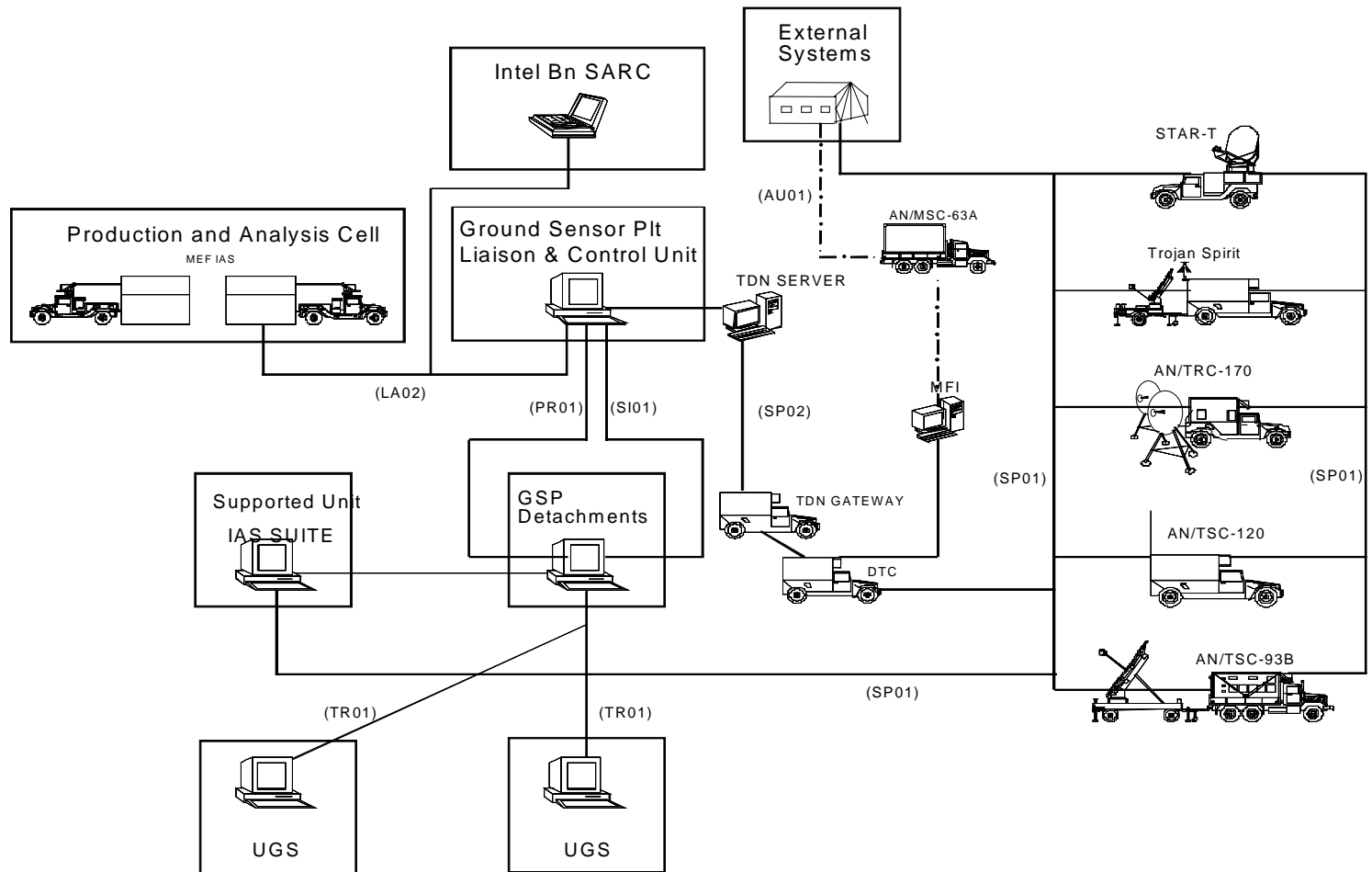


Figure I-10. Ground Sensor Platoon, Intelligence Battalion, Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	IAS .V2		
Intel Ops/C2 Node	Supported Unit	SARC	SARC
Ground Sensor Plt Dets TRSS monitoring			
Comm Net			
Direction	B	B	B
Comm Links	LA02	SI01	PR01
Internal Message Format	SENREP (USMTF)	SENREP (USMTF)	SENREP (USMTF)

Table I-10. Ground Sensor Platoon Systems and Communications Interface Requirements

* Shows GENSER Secret connections.
SCI connections shown in Figure I-12.



MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS.	IAS V2	IAS V1	IAS IOW	IAS V2	IAS V2	JSWS
Intel Ops/C2 Node	MEF	Div	Regt	Bn	FSSG	Wing	Div
IAS V2							
Comm Net							
Direction	B	B	B	B	B	B	R
Comm Links	SP01	LA01	SP01	EP01	SP01	SP01	DL01
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	NITF Imagery
Comm Net							
Direction	B		B	B	B	B	
Comm Links	PS01-02		PS01-02	PS01-02	PS01-02	PS01-02	
Internal Message Format	OTH-G, USMTF, VMF		OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	
Comm Net							
Direction	B		B	B			
Comm Links	SI01		SI01	SI01			
Internal Message Format	OTH-G, USMTF, VMF		OTH-G, USMTF, VMF	OTH-G, USMTF, VMF			
Comm Net							
Direction	B		B	B			
Comm Links	PR01		PR01	PR01			
Internal Message Format	OTH-G, USMTF, VMF		OTH-G, USMTF, VMF	OTH-G, USMTF, VMF			

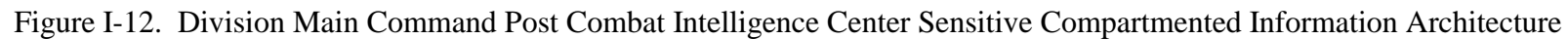
Table I-11. Division Main Command Post CIC GENSER Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

Systems	CTT/JTT	TCO	AFATDS	DTAMS	MANPACK SIDS	CIHEP	TRSS
Intel Ops/C2 Node	Div	Div	Div	Div	Direct Support	Direct Support	Direct Support
IAS V2							
Comm Net							Sensor Net
Direction	R	B	B	R	R	R	R
Comm Links	TT01-04, & IB01	LA02	LA02	LA02	VI01	VI01	PR01 / SI04
Internal Message Format	TADIL-J and VMF	OTH-G, USMTF	OTH-G, USMTF, VMF	CADRG, ADRG, JPEG, VPF, NITF	NITF Imagery	NITF Imagery & Tape	SENREP (USMTF)

Table I-11. Division Main Command Post CIC GENSER Systems and Communications Interface Requirements (cont.)

- 1
- 2
- 3
- 4



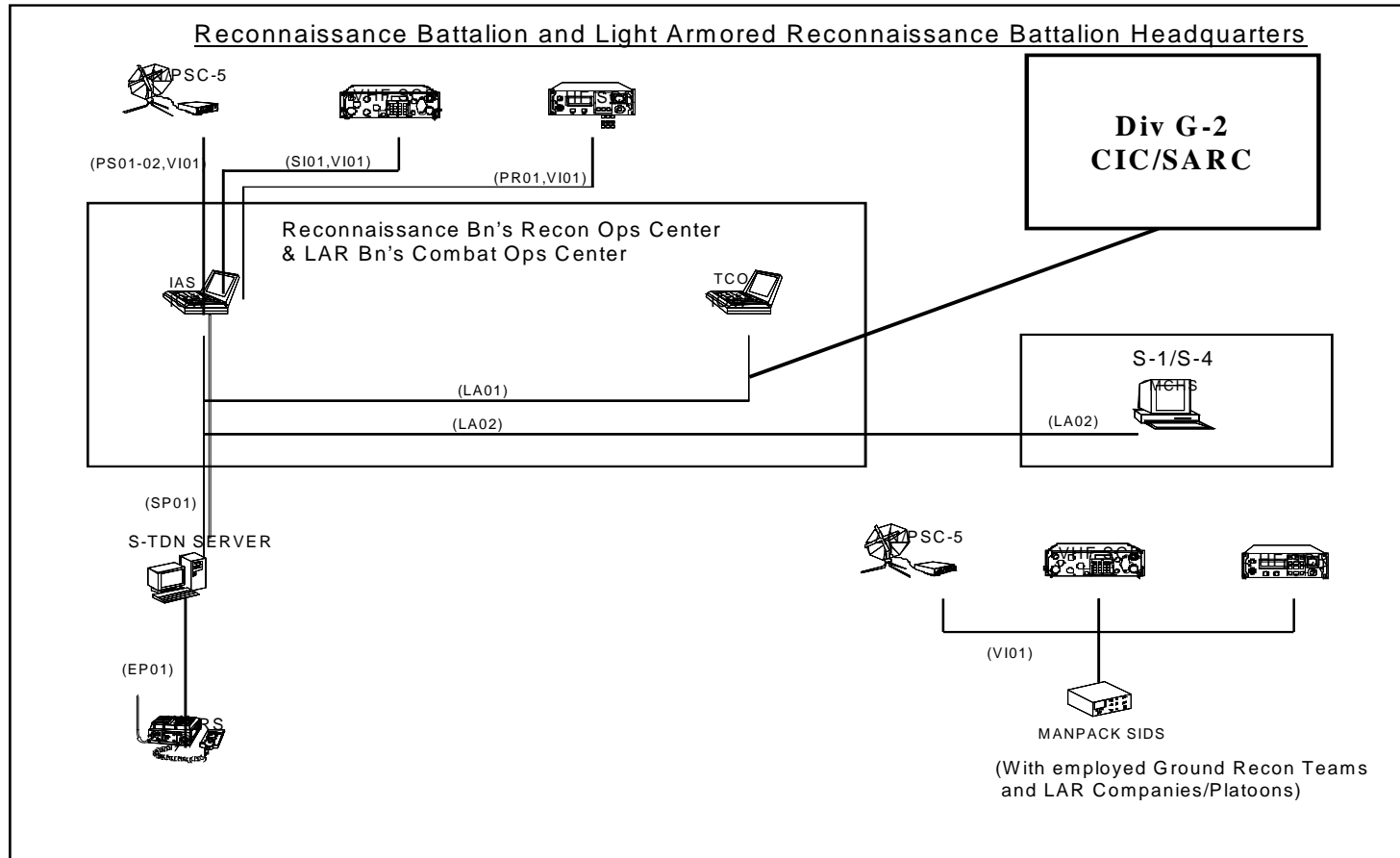
MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS.	IAS V2	IAS V2	CTT/JTT	External Commands (SCI)
Intel Ops/C2 Node	MEF (SCI)	Div (SCI)	Wing (SCI)	Div (SCI)	
IAS V2					
Comm Net					
Direction	B	B	B	R	B
Comm Links	JW02	LA01	SP01	TT01-04, & IB01	JW02
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, VMF	OTH-G, USMTF, VMF	TADIL-J and VMF	USMTF, VMF
Comm Net					
Direction	B		B		
Comm Links	PS01-02		PS01-02		
Internal Message Format	OTH-G, USMTF, VMF		OTH-G, USMTF, VMF		
Comm Net					
Direction	B		B		B
Comm Links	AU02		AU02		AU02
Internal Message Format	OTH-G, USMTF		OTH-G, USMTF		OTH-G, USMTF
Comm Net					
Direction	B				
Comm Links	SI01				
Internal Message Format	OTH-G, USMTF, VMF				

Table I-12. Division Main Command Post CIC SCI Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

1



2

3

4

5

Figure I-13. Reconnaissance Battalion Reconnaissance Operations Center and Light Armored
Reconnaissance Battalion Combat Operations Center Architectures

MCWP 2-13
COORDINATING DRAFT

1

Systems	IAS V2	IAS V1	TCO IOW	MANPACK SIDS	CIHEP	TRSS
Intel Ops/C2 Node	Div	Regt	Bn	Direct Support	Direct Support	Direct Support
IAS IOW						
Comm Net						Sensor Net
Direction	B	B	B	R	R	R
Comm Links	PS01-02	EP01	LA01	VI01	VI01	PR01 / SI04
Internal Message Format	OTH-G, USMTF, VMF, VDX	OTH-G, VMF, VDX	OTH-G, USMTF, VMF, VDX	NITF Imagery	NITF Imagery & Tape	SENREP (USMTF)
Comm Net						
Direction	B	B				
Comm Links	SI01	PS01-02				
Internal Message Format	OTH-G, USMTF, VMF, VDX	OTH-G, USMTF, VMF, VDX				
Comm Net						
Direction	B	B				
Comm Links	PR01	SI01				
Internal Message Format	OTH-G, USMTF, VMF, VDX	OTH-G, USMTF, VMF, VDX				
Comm Net						
Direction		B				
Comm Links		PR01				
Internal Message Format		OTH-G, USMTF, VMF, VDX				

2

3

4

5

6

Table I-13. Reconnaissance Battalion Reconnaissance Operations Center and Light Armored
Reconnaissance Battalion Combat Operations Center Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

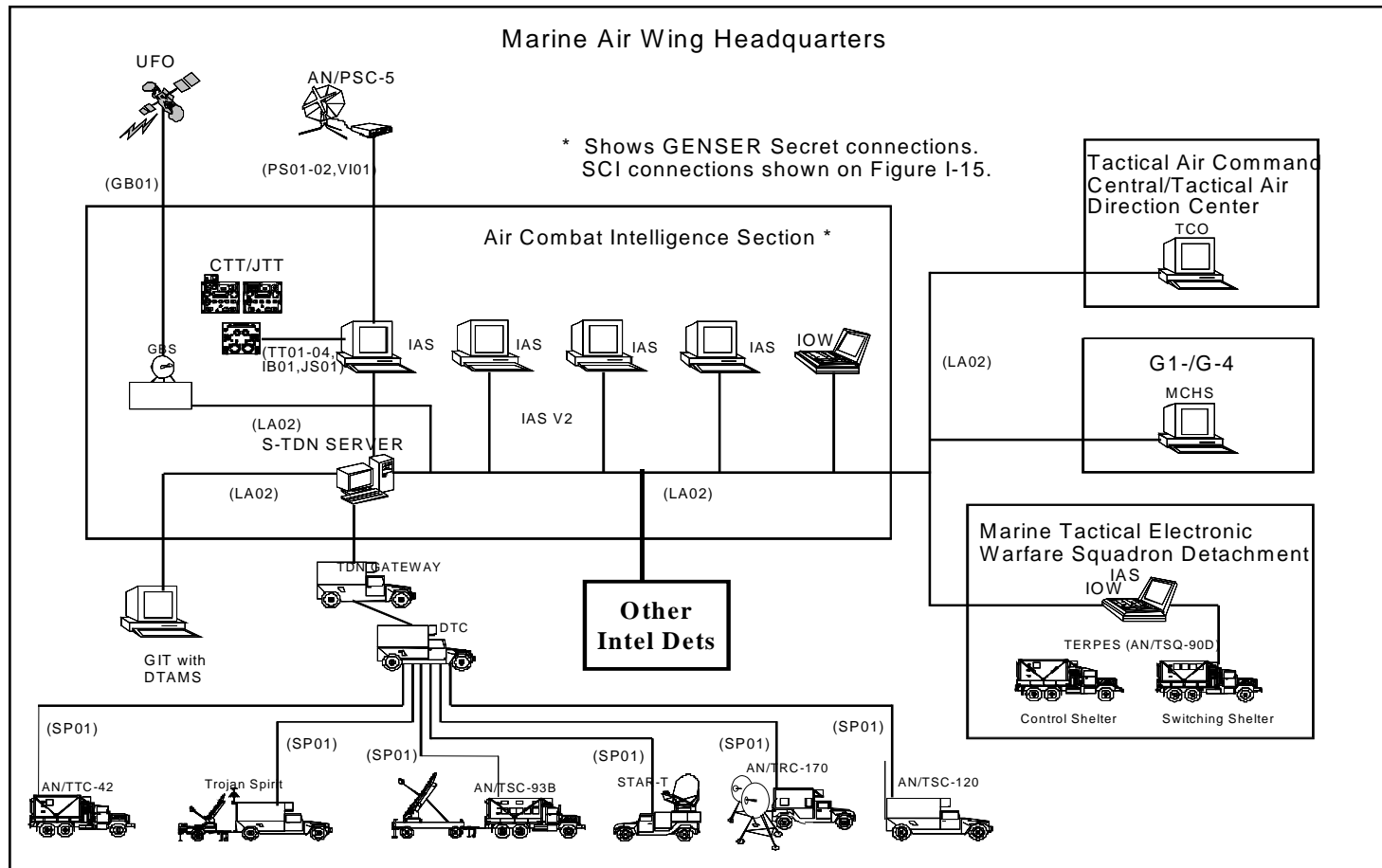


Figure I-14. Marine Aircraft Wing Air Combat Intelligence Section GENSER Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS.	IAS V2	IAS V2	IAS V2	IAS V2	IAS IOW	TCO	IOW	DTAMS
Intel Ops/C2 Node	MEF	Wing	MAG	Div	FSSG	Squadron	Wing	VMAQ	TOPO GIST
IAS V2									
Comm Net									
Direction	B	B	B	B	B	B	B	B	B
Comm Links	SP01	LA01	SP01	SP01	SP01	SP01	LA02	LA02	LA02
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF, VDX	OTH-G, USMTF, VMF	VDX, OTH-G, USMTF, VMF	OTH-G, USMTF, VMF, CADRG,GE OTIF,VPF & OTHERS
Comm Net									
Direction	B								
Comm Links	PS01-02								
Internal Message Format	OTH-G, USMTF, VMF								

Table I-14. Marine Aircraft Wing Air Combat Intelligence Section GENSER Intelligence Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

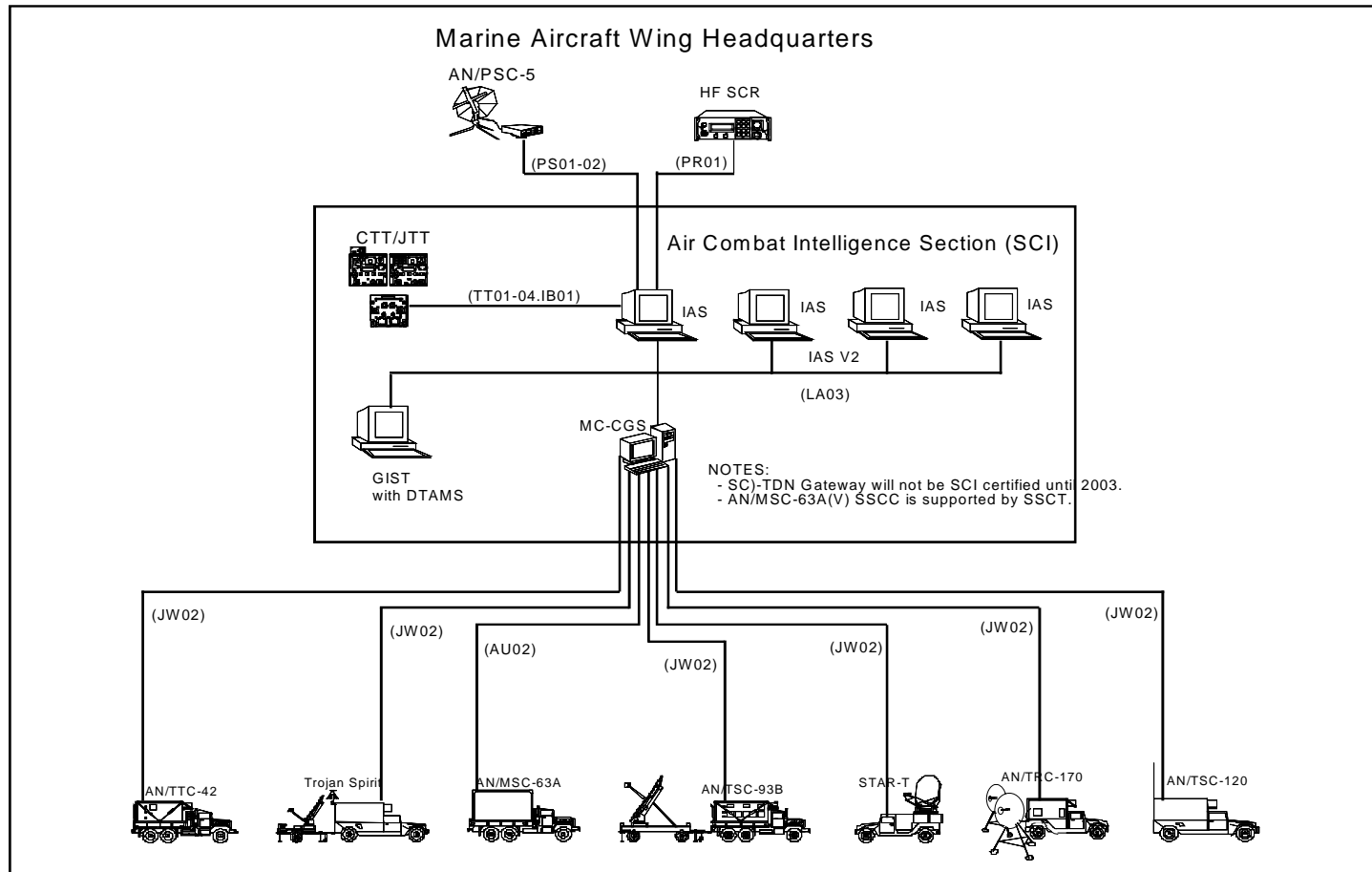


Figure I-15. Marine Aircraft Wing Air Combat Intelligence Section SCI CIS Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	IAS V2	IAS V2	IAS V2	IAS V2	DTAMS
Intel Ops/C2 Node	MEF	Wing	Div	FSSG	TOPO GIST
IAS V2					
Comm Net					
Direction	B	B	B	B	B
Comm Links	JW02	LA01	JW02	JW02	LA02
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF, CADRG, GEOTIF, VPF & OTHERS

Table I-15. Marine Aircraft Wing Air Combat Intelligence Section SCI Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

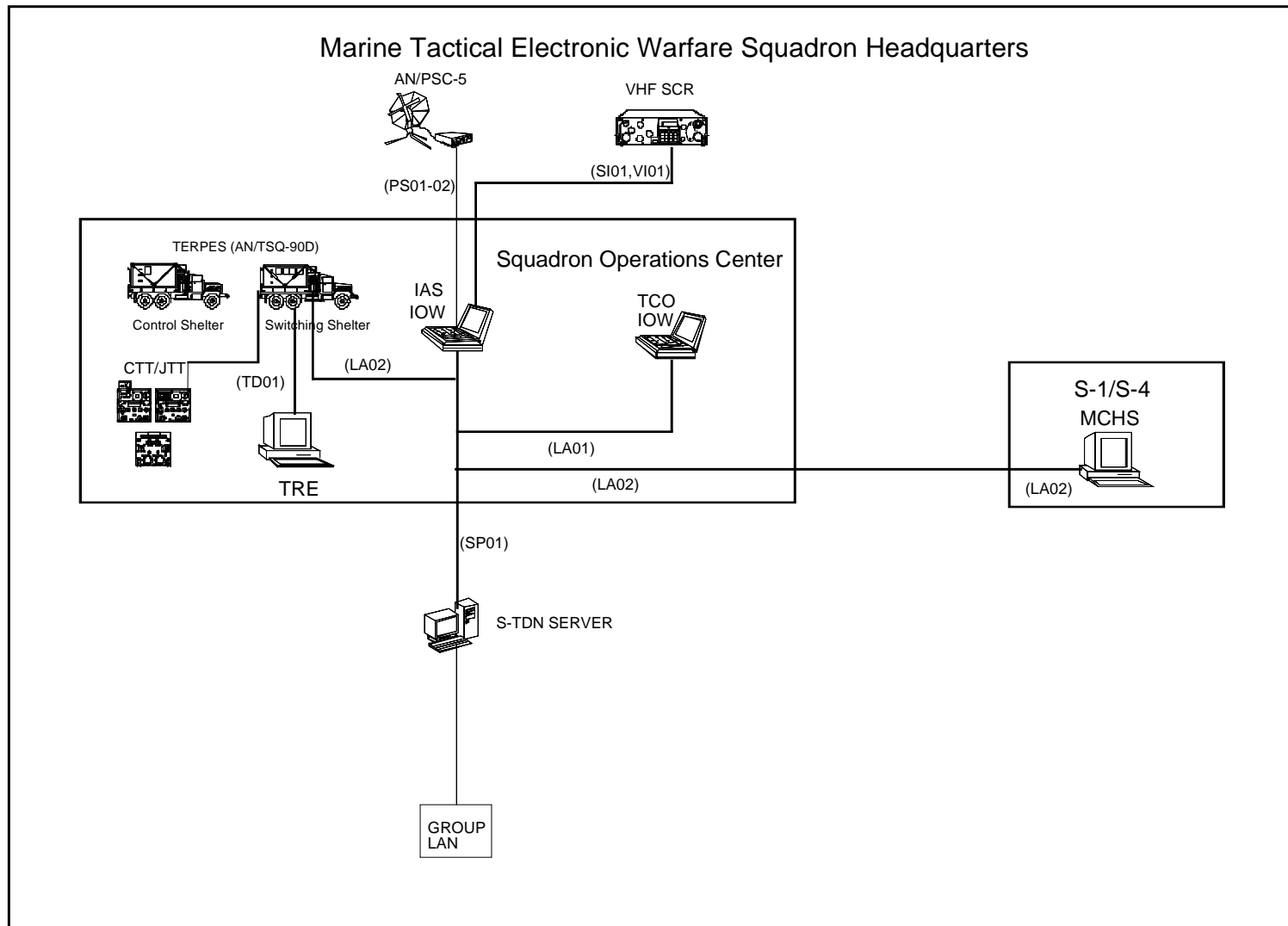


Figure I-16. VMAQ Squadron Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	IAS V2	IAS IOW	TCO	CTT/JTT to TERPES	TRE to TERPES
Intel Ops/C2 Node	MAG	Squadron	Squadron	Squadron	Squadron
IAS IOW					
Comm Net					
Direction	B	B	B	R	R
Comm Links	SP01	LA01		TT01-04, & IB01	TT01-
Internal Message Format	VDX	VDX	VDX	TADIL-J and VMF	TADIX-B

Table I-I6. VMAQ Squadron Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

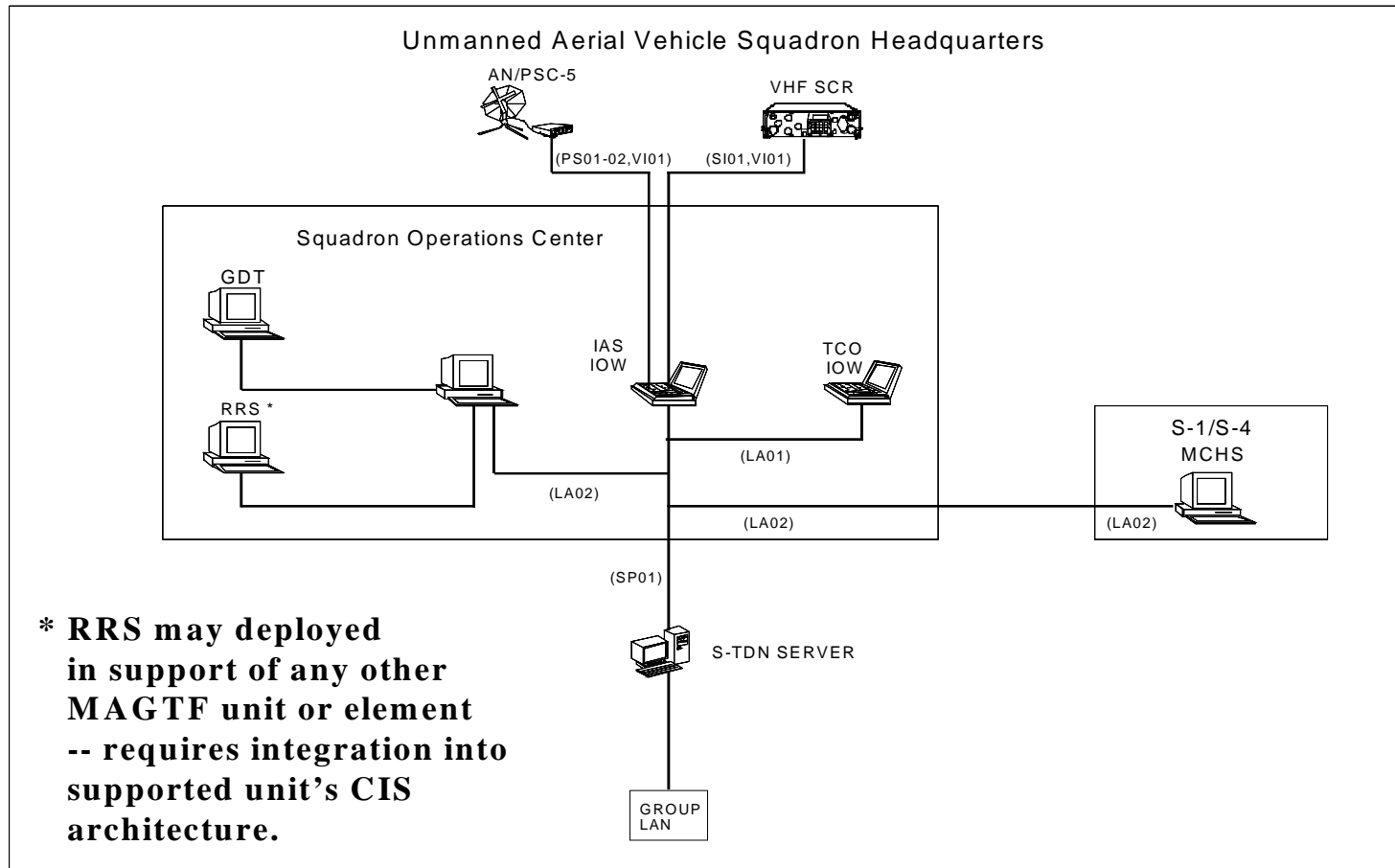


Figure I-17. VMU Squadron Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	IAS V2	IAS IOW	TCO	TCS	UAV to TCS
Intel Ops/C2 Node	MAG	Squadron	Squadron	Squadron	Squadron
IAS IOW					
Comm Net					
Direction	B	B	B	B	B
Comm Links	SP01	LA01		LA02	TC01
Internal Message Format	VDX, NITF	VDX, NITF	VDX, NITF	NITF	Imagery, SAR, I/R, E/O

Table I-17. VMU Squadron Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

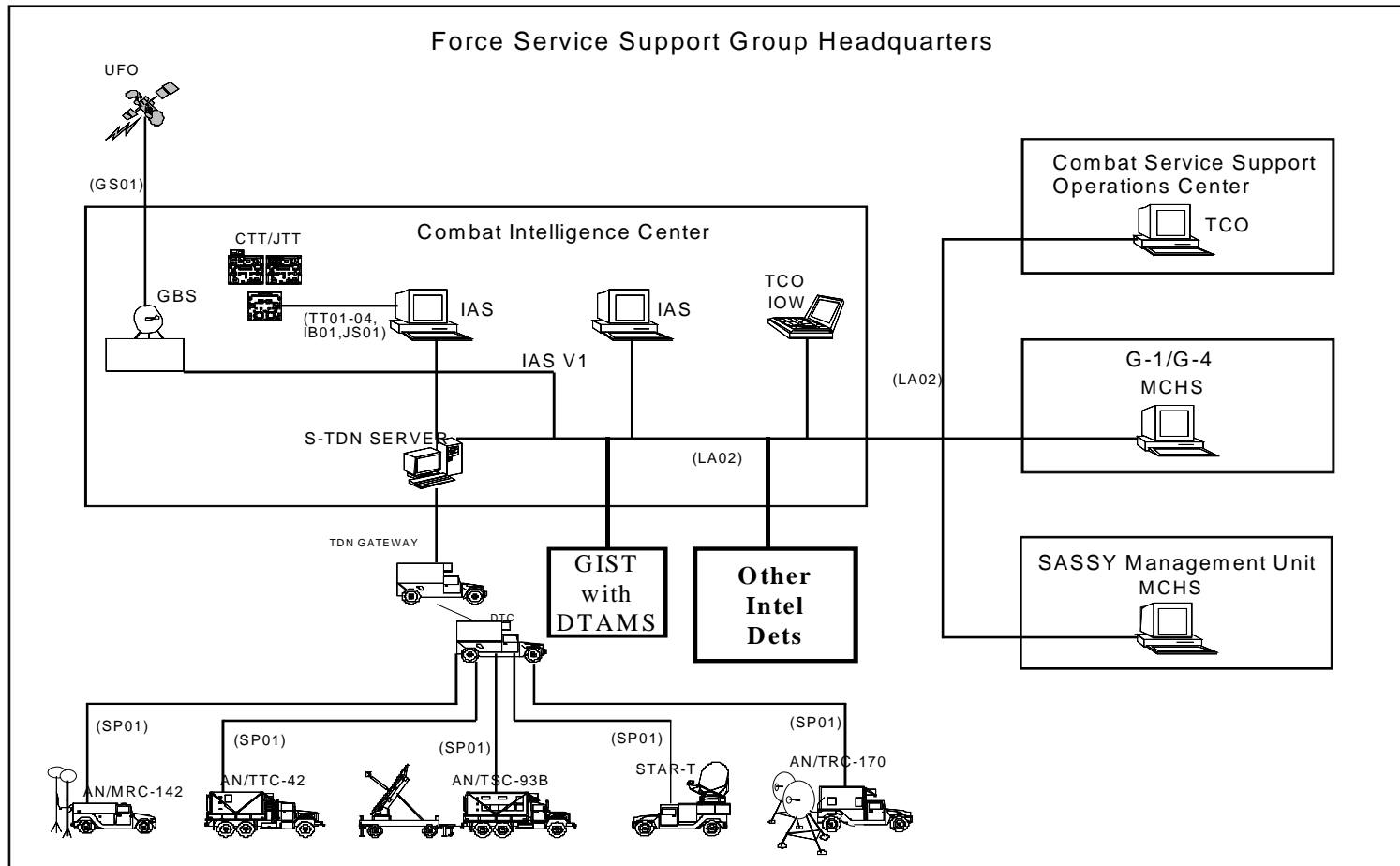


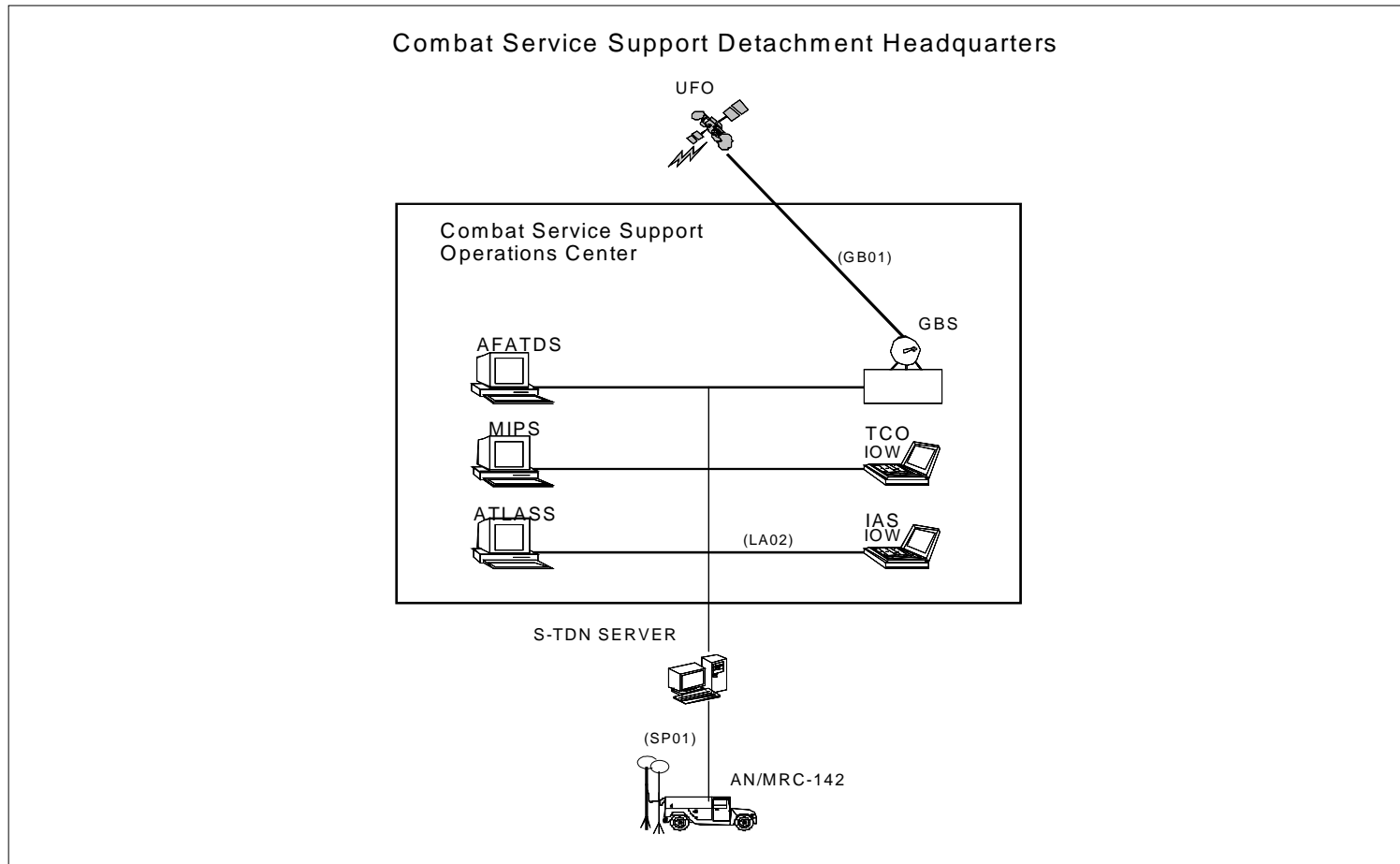
Figure I-18. FSSG Headquarters Combat Intelligence Center Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	MEF IAS	IAS V2	IAS V2	IAS V2	IAS IOW	TCO	CTT/JTT	DTAMS
Intel Ops/C2 Node	MEF	Wing	Div	FSSG	CSSD	FSSG	FSSG	Topo GIST
IAS V2								
Comm Net								
Direction	B	B	B	B	B	B	R	B
Comm Links	SP01	SP01	SP01	LA01	SP01	LA02	TT01-04, & IB01	LA02
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	VDX, OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	TADIL-J and VMF	OTH-G, USMTF, VMF, CADRG, GEO TIF, VPF & OTHERS

Table I-18. FSSG CIC Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT



1
2
3
4

Figure I-19. Combat Service Support Detachment Architecture

MCWP 2-13
COORDINATING DRAFT

Systems	IAS V2	IAS IOW V1	TCO IOW
Intel Ops/C2 Node	FSSG	CSSD	CSSD
IAS IOW			
Comm Net			
Direction	B	B	B
Comm Links	PS01-02	EP01	LA01
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, VMF	OTH-G, USMTF, VMF
Comm Net			
Direction	B	B	
Comm Links	SI01	PS01-02	
Internal Message Format	OTH-G, USMTF, VMF	OTH-G, USMTF, VMF	

Table I-19. Combat Service Support Detachment Systems and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

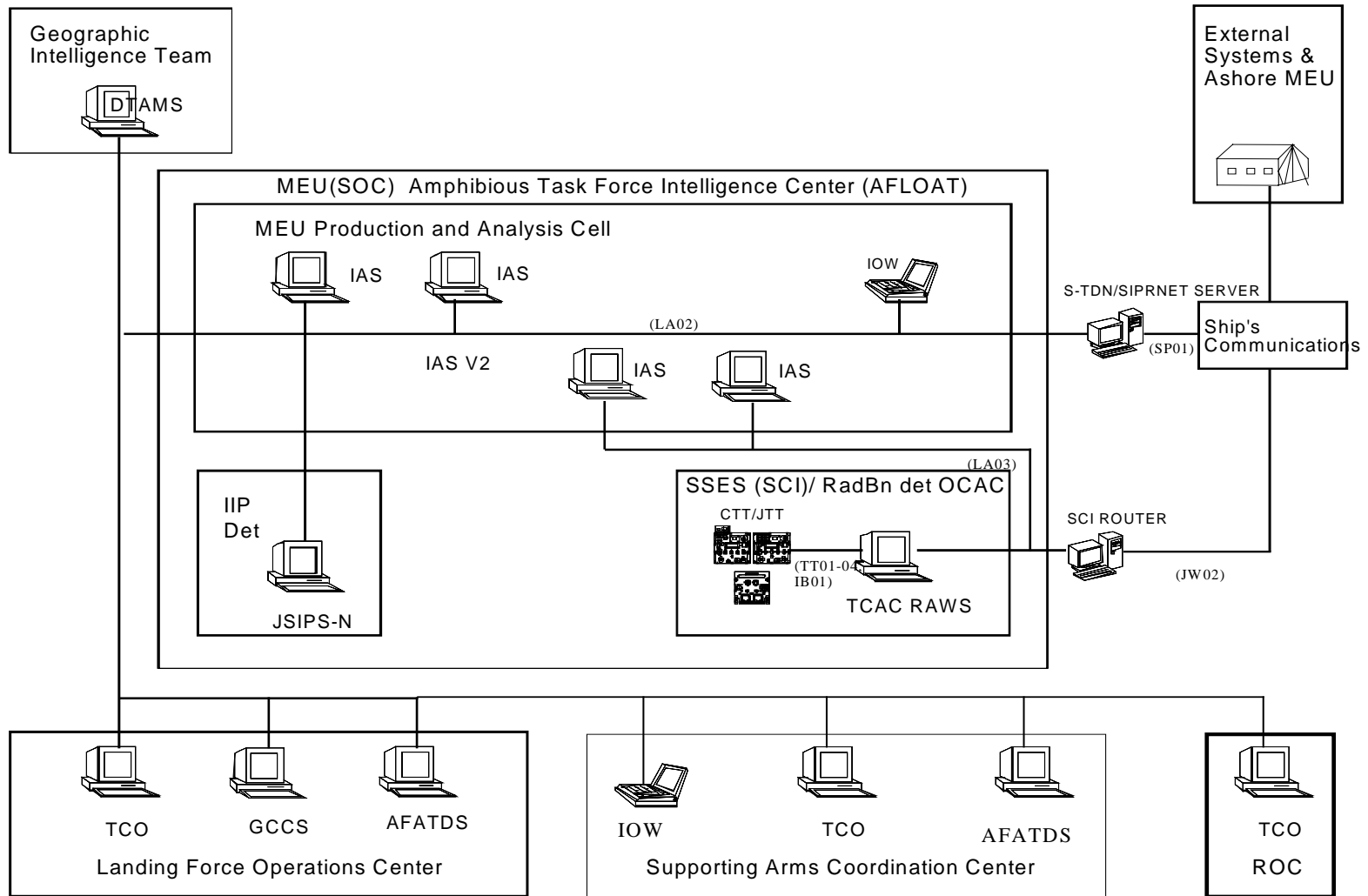


Figure I-20. MEU(SOC) Amphibious Task Force Intelligence Center CIC Architecture (Afloat)

MCWP 2-13
COORDINATING DRAFT

Systems	IAS V2	IOW	DTAMS	JSIPS-N	TCO	IOW
Intel Ops/C2 Node	P&A Cell	P&A Cell	GIT	IIP Det	LFOC	SACC
IAS V2						
Comm Net						
Direction	B	B	B	B	B	B
Comm Links	LA02	LA02	LA02	LA02	LA02	
Internal Message Format	OTH-G, USMTF, VMF	VDX	OTH-G, USMTF, VMF, CADRG, GEOTIF, VPF & OTHERS	NITF.2, USMTF	OTH-G, USMTF, VMF, NITF	OTH-G, USMTF, VMF, NITF
Intel Ops/C2 Node	LFOC	LFOC	EXTERNAL & ASHORE MEU SYSTEMS			
Systems	GCCS	AFATDS				
Comm Net						
Direction	B	B	B			
Comm Links	LA02	LA02	SP01			
Internal Message Format	USMTF, VMF	USMTF, VMF	OTH-G, USMTF, VMF, NITF			

Table I-20. MEU(SOC) ATFIC CIC GENSER System and Communications Interface Requirements

Systems	CCT/JTT	EXTERNAL & ASHORE MEU SYSTEMS
Intel Ops/C2 Node	RadBn OCAC/SSES	
TCAC RAWS		
Comm Net		Via MC GCS or other router
Direction	R	B
Comm Links	TT01-04, & IB01	JW02
Internal Message Format	TADIL-J and VMF	USSID, USMTF, VMF, NITF

Table I-21. MEU(SOC) ATFIC CIC SCI System and Communications Interface Requirements

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
AN/PRC-104/ AN/MRC-213 or AN/MRC-231 (HF) (PR01)	Radio Cabling	Host controlled	Host controlled	Host controlled	Host controlled			TSEC/KY-99A MINTERM	AN/PRC-104/ AN/MRC-213 or AN/MRC-231 (HF)	The KY-99 can act as a modem
AN/PSC-5 (UHF) DAMA 5 Khz (PS03)	Radio Cabling	MIL-STD 188-220A				TCIM				Used with TPCS
AN/PSC-5 (UHF) DAMA 25 Khz (PS04)	Radio Cabling	MIL-STD 188-220A				TCIM				Used with TPCS
AN/PSC-5 (UHF) DAMA 25 Khz (PS02)	Radio Cabling	Host controlled	Host controlled	Host controlled	Host controlled	Imbedded, but can operate with external		ICOM COMPATIBLE W/KYV-5, KG- 84A KY-5 &KY- 99(ANDVT		Allows nominal 16Kbps transmission
AN/PSC-5 (UHF) DAMA 5 Khz (PS01)	Radio Cabling	Host controlled	Host controlled	Host controlled	Host controlled	Imbedded, but can operate with external		ICOM COMPATIBLE W/KYV-5, KG- 84A KY-5 &KY- 99(ANDVT	AN/PSC-5	Allows external encrypted operation w/KL-43C. Nominal 4.8 & 9.6 Kbps
AN/VRC-99 (UHF) MECDL (ME01)	Radio cabling				IEWCOM CAT/ USMTF					AN/VRC-99 Must be provided at both origination and destination site

2

3

4

5

Table I-22. Standard Communication Pathways and Connectivity

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
AUTODIN (AU01)	RS-232, RS-442, or MIL-STD-188-114	Mode I			DOI-103 Or JANAP 128	TLC-10 or replacement		KG-84, KIV-7 OR EQUIVALENT		This will only be an SCI net when the TCCs are phased out
AUTODIN (AU02)	RS-232, RS-442, or MIL-STD-188-114	Mode II			DOI-103			KG-84, KIV-7 OR EQUIVALENT		This net may continue to be used for lower level USMTF messages.
CDL (CD01)	TGDL/STLS OC-3c SONET	ATM			CIGSS ICD-F/A-18-064				TGDL 137 MHz HR RL 2 channels @42.84 MHz	Data in TIGDL-SI-101 Interface Specification Used for ATARS, ASARSII & SYERS
Direct Link (DL01)	RS-232				NITF					
EPLRS (EP01)	Via LAN	X.25	Internet Protocol	Transport Control Protocol	SMTP, DMS, VMF		TDN Server or TDN Gateway	TSEC/ KGV-13 ICOM	EPLRS	LAN connection via TDN
EPLRS (EP02)	EPLRS ADDSI (X.25 Subset) or MIL-STD-1553B	X.25	Internet Protocol	Transport Control Protocol	SMTP, DMS, VMF	External to EPLRS		TSEC/ KGV-13 ICOM	EPLRS	Direct connection to EPLRS

2

3

4

5

Table I-22. Standard Communication Pathways and Connectivity (cont.)

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
EPLRS (EP03)	EPLRS ADDSI (X.25 Subset) or MIL-STD-1553B	MIL-STD-188-220B	Internet Protocol	Transport Control Protocol	VMF	External to EPLRS must be MIL-STD-188-220B Compliant		TSEC/ KGV-13 ICOM	EPLRS	MIL-STD-188-220B
GBS	Via LAN	IEEE 802.3 Ethernet	Internet Protocol	Transport Control Protocol	MPEG-2, SMTP, FTP, NTSC		TDN via IP address	KG-75 TACLANE and FAST LANE	UFO	All imagery converted to MPEG-2, Video is DVB converted to NTSC
HAVE QUICK AN/VRC- 83 (HQ01)	Need additional research							TSEC/KY-57 HYP-57/TSEC		
IBS (IB01)	JTT				TADIL-J or VMF			KG-11 Embedded		The TADIX-B format will be translated into either TADIL J or VMF at the user's direction
Joint Stars (JS01)	To be determined									
JWICS (JW01)	Via LAN	IEEE 802.3	Internet Protocol	Transport Control Protocol	SMTP/ FTP		TDN Server or TDN Gateway	KIV-7	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future. Cannot Be done until TDN is SCI certified

2

3

Table I-22. Standard Communication Pathways and Connectivity (cont.)

4

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
JWICS (JW02)	RS-232, RS-442, or MIL-STD-188-114	PPP, SLIP, 802.3	Internet Protocol	Transport Control Protocol	SMTP/FTP		CGS-100 or other than TDN	KIV-7	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future
LAN (LA01)	10-BASE-T 10-BASE-5 10-BASE-2 100-BASE-T	Ethernet IEEE 802.3			N/A					Directly linked system
LAN (LA02)	10-BASE-T 10-BASE-5 10-BASE-2 100-BASE-T	Ethernet IEEE 802.3	Internet Protocol	Transport Control Protocol	SMTP FTP					Indirectly linked system
LAN (LA03)	10-BASE-T 10-BASE-5 10-BASE-2 100-BASE-T	Ethernet IEEE 802.3	Internet Protocol	Transport Control Protocol	SMTP FTP					SCI Version of LA02
NIPRNET (NP01)	Via LAN	IEEE 802.3	Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP		TDN Server or TDN Gateway		AN/TSC-85/93, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future
NIPRNET (NP02)	RS-232, RS-442, or MIL-STD-188-114	PPP, SLIP, OTHER?	Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP				AN/TSC-85/93, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future

2

3

Table I-22. Standard Communication Pathways and Connectivity (cont.)

4

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
SCDL (SC01) (UP-LINK)	Integrated ADT				C2 Msgs			KGV-8	Ku ADT	
SCDL (SC02) (DOWN-LINK)	Integrated GDT				Real Time MTI/FTI/SAR			KGV-8	Ku GDT	The GDT receives the data at the CGS
SINCGARS (SI03)	RS-232, RS-442, or MIL-STD-188-114	LAP B	X.25 & Internet Protocol	Transport Control Protocol	SMTP	TCIM		TSEC/KY-57 ICOM	SINCGARS	
SINCGARS (SI04)	RS-232, RS-442, or MIL-STD-188-114	Mode 11			DOI-103 or JANAP 128			TSEC/KY-57 ICOM	SINCGARS	Traffic can still be passed with this configuration. It is very similar to radio teletype
SINCGARS (SI05)		See SDD VOL 2	Apache Long Bow	MSIP 000260-104		IDM				
SINCGARS (SI01)	RS-232, RS-442, or MIL-STD-188-114	MIL-STD-188-220B	MIL-STD-2045-47001/Internet Protocol	Transport Control Protocol	VMF	Host must provide.		TSEC/KY-57 ICOM	SINCGARS	Host modem must provide the MIL-STD 188-220B protocol and modem
SINCGARS (SI02)	RS-232, RS-442, or MIL-STD-188-114	MIL-STD-188-220A	Internet Protocol	Transport Control Protocol	MTS B, SMTP	TCIM		TSEC/KY-57 ICOM	SINCGARS	

2

3

Table I-22. Standard Communication Pathways and Connectivity (cont.)

4

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
SIPRNET (SP01)	Via LAN	IEEE 802.3 on LAN, LAP-B for X.25, or PPP	X.25 & Internet Protocol, or Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP		TDN Server or TDN Gateway	KIV-7	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. STAR-T & SMART-T in the future
SIPRNET (SP02)	Via LAN	IEEE 802.3 on LAN, LAP-B for X.25, or PPP	X.25 & Internet Protocol, or Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP		CGS-100 or other than TDN	KIV-7 or compatible	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future
SIPRNET (SP03)	Via LAN	IEEE 802.3 on LAN, LAP-B for X.25, or PPP	X.25 & Internet Protocol, or Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP		CGS-100 or other than TDN	KIV-7 or compatible	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future Used in SCIF
SIPRNET (SP04)	RS-232, RS-442, or MIL-STD-188-114	PPP, SLIP, OTHER?	Internet Protocol	Transport Control Protocol	SMTP/DMS/FTP		CGS-100 or other than TDN	KIV-7HS	AN/TSC-85/93, TS II, or DISN STEP	Transmission source may vary. . STAR-T & SMART-T in the future
TADIX-B (TT01)	CTT/H3/TRUE				TADIX-B					No plans to convert to IBS
TDDS (TT03)	CTT/H3/JTT	TDD Unique See CTT ICD A3111338-003970			Similar to TADIX-B			KGV-11 Embedded	FLTSATCOM or UFO	Will be converted to IBS
TIBS (TT04)	CTT/H3/JTT	TDMA			Bit-oriented Unique			KGV-11 Embedded	UHF Satellite	Will be converted to IBS

2

3

Table I-22. Standard Communication Pathways and Connectivity (cont.)

4

MCWP 2-13
COORDINATING DRAFT

1

Designator	Physical Connection	Datalink	Network	Transport	Message Header Format	Modem	Switch or Server	Crypto	Transmitter	Remarks
TRIXS (TT02)	CTT/H3/JT T	TDMA using HAVE QUICK II algorithm			USMTF			KGV-11 Embedded	GR/CS and CARS	Will be converted to IBS
UAV Video (UA01)	RS-170				Video					I have to determine how to transmit this image
UAV Telemetry (UA02)	RS-422				UAV Telemetry					
VIASAT (VI01)	Radio cabling	PROCOMM & Various others			HUIT & Various others	VIASAT				The VIASAT has been tested using SINCGARS, HF and UHF SCR

2

3

Table I-22. Standard Communication Pathways and Connectivity (cont.)

4

MCWP 2-13
COORDINATING DRAFT

Section II

MAGTF Intelligence, Counterintelligence and Reconnaissance Radio Nets

Introduction. The MEF Master Net List is a database that facilitates the *MEF's Revised Battlefield Electronic CEOI System* CEOI generation. These files are unclassified and consist of every circuit within the MEF and each circuit's emission requirements, as well as grouping, call sign, and call word information. The MEF Master Net List is controlled by the MEF G-6 and is managed by the MEF frequency manager. The MEF Master Net List will be reviewed annually for proposed modifications on the basis of input from commanders. Requests for modification of the Master Net List will be submitted to higher HQ for consolidation and review. The Master Net List, and thereby CEOI net assignments, should not be modified without the review and approval of the MEF AC/S G-6.

The need to maintain consistent, standard radio network terminology demands that MEF radio circuit assignments be regulated. With the introduction of the Revised Battlefield Electronic CEOI System Master Net List, electronic CEOI information can be matched to the task organization, edited, generated, and printed for an entire MEF within hours. Unit participation in Master Net List revisions and compliance are essential to maintaining the currency of this information.

Table I-23. Special Characteristics of the Master Net List

Item	Purpose	Comment
Net number	Reference	Used to provide task organization requirements to higher HQ
Net name	Description	Standard net description
Net ID	SINCGARS	000 - 999
Call sign	Call-sign assignment	Yes or No, assigned randomly
Organizational code	Echelon separation	Allows for duplicate net IDs within separate units
Restrictions	Sub-band separation	Allows for restrictive frequency assignments (such as HF day and night)
Frequency	Band assignment	N=None, H=HF, F=VHF, A=VHF-AM, U=UHF, S=SHF, E=EHF
Power	Output power	1-High through 4-Low
Reuse class	Geographic separation	Strategic
Reuse zone	Sub-geographic separation	Tactical
Call word	Call-word assignment	Fixed or random

MCWP 2-13
COORDINATING DRAFT

The following information is an extract showing intelligence, reconnaissance and select key other radio nets that may be established for any operation. It is a planning guide for radio nets that may be established to satisfy MAGTF intelligence CIS radio requirements. As with all intelligence CIS architecture matters, the specific radio nets, operational and functional descriptions, what bands are used, net composition, etc., will be heavily influenced by METT-T, the commander's guidance, concepts of operations, and task-organizations. For the MEF the CMDO officer, assisted by the intelligence systems officer, SARC OIC, and intelligence and reconnaissance units commanders/OICs, is responsible for planning and coordinating radio net support of MEF intelligence, CI and reconnaissance operations. With subordinate unit intelligence section, the intelligence operations officer/air combat intelligence officer usually is responsible for this.

The kinds of services (voice, video, facsimile, data, imagery, etc.) that are required should be determined and adjusted to conform to available resources (personnel, equipment, and frequency/channel availability) and environmental characteristics. The required service will be governed primarily by the tactical situation, terrain features, and distances between stations on the net (with due consideration to equipment inventories and available personnel). Multiple nets of the same type may be established to handle excess traffic volume. These nets would have a number suffix such as 1, 2, and 3 for the primary, secondary, and tertiary circuits of the same type. The primary net descriptions are given in this section.

Within each net composition, units in *italics* normally participate in the specified net as required. There is no absolute requirement for each unit noted to participate in net composition. Intelligence operations planners and unit CIS officers can use the net composition in this appendix for planning and compiling radio guard charts for operations. Where multiple frequency bands are listed in parentheses following radio net titles, the frequency band that is normally assigned is listed first.

1. Marine Air-Ground Task Force Command Element Intelligence, Counterintelligence and Reconnaissance Nets.

MAGTF CE nets are established to support the exercise of command and control during combat operations. The type operation, commander's intent, concept of operations, environment, enemy capabilities, and MAGTF task organization will influence which nets are required and established. During amphibious operations the term MAGTF is synonymous with the term landing force. MAGTF CE nets include the following:

MCWP 2-13
COORDINATING DRAFT

a. MAGTF Ground Reconnaissance Command (UHF-SATCOM/HF). Used for command and control of landing force ground reconnaissance operations and transmission of collected reconnaissance directly to the MAGTF commander or the MAGTF CE combat intelligence center (CIC).

w CE

w organic and direct support reconnaissance units

w Unmanned aerial vehicle (UAV) squadron/detachment

w GCE(s)

w *Other units, as required (e.g. radio battalion radio reconnaissance team (RRT), Navy special warfare teams, etc.)*

b. MAGTF Alert/Broadcast (HF). Used for alert warning traffic or general traffic pertaining to all (or the majority) of the units on this net. Messages not of an alert warning type will be consecutively numbered upon transmission.

w CE

w *Designated units within the MAGTF major subordinate element(s)*

c. MAGTF Intelligence (UHF-SATCOM/HF/VHF). Used for rapid reporting and dissemination of intelligence, collaborative planning of future MAGTF intelligence operations, and command and control of ongoing MAGTF intelligence and reconnaissance operations.

w CE

w GCE(s)

w ACE(s)

w CSSE

w Organic and direct support intelligence and reconnaissance units

w UAV squadron/detachment

MCWP 2-13
COORDINATING DRAFT

d. MAGTF Air Observation (UHF/VHF). Used to coordinate air observation and transmit information from air observers to MAGTF elements. May be used to adjust artillery or naval gunfire (NGF) on an emergency basis.

- w CE
- w Aerial observer
- w GCE
- w FSCCs
- w *Artillery battery FDC*
- w *Supporting arms special staff (SASS)*

e. MAGTF EW Coordination (HF). Used to coordinate electronic attack (EA) and SIGINT activities.

- w CE (G-3/S-3 EWCC)
- w OCAC
- w GCE
- w TACC
- w TAOC

f. MAGTF Defense Special Security Communications System (DSSCS) Entry (UHF-SATCOM/HF/Multiplex (MUX)).
Used to provide the MAGTF commander with an SCI data communication capability with external agencies. The communication path is usually provided by the supported commander (i.e., communications battalion or detachment), and the terminal equipment and personnel are provided by the radio battalion/SIGINT support unit (SSU) special security communications element (SSCE).

- w MAGTF CE via the radio battalion/detachment special security communication element

MCWP 2-13
COORDINATING DRAFT

g. MAGTF Special Intelligence Communications Net External (HF). Used to provide the MAGTF commander with a secure data communications channel for the exchange of SCI. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion SSCE.

- w MAGTF CE via the radio battalion/SSU special security communication element
- w CJTF
- w CATF

h. MAGTF Critical Communications (CRITICOMM) Net (UHF-SATCOM/VHF). Used to provide the supported commander with a channel to adjacent Service cryptologic agencies or cryptologic support group. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/SSCE.

- w MAGTF CE via the radio battalion/SSU SSCE
- w Higher HQ, adjacent HQ, and theater and national intelligence/SIGINT agencies

i. MAGTF Internal Special Intelligence Communications Handling System Net (VHF/UHF/SHF). Used to provide the MAGTF commander with a secure SCI communications capability with subordinate division/wing commanders through their organic SSCT. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/SSU SSCE.

- w MAGTF CE via radio battalion/SSU SSCE
- w Division Special Security Communications Team (SSCT)
- w MAW SSCT

j. Radio Battalion/SSU Command and Control Net (HF/VHF). Used to provide the battalion commander/detachment officer in charge with command and control of subordinate elements. The communications path, equipment, and personnel are provided by the radio battalion.

- w Radio battalion operations control and analysis center (OCAC)
- w Radio battalion OCAC liaison teams (OLT), company command elements (CCE), SIGINT support platoons (SSP), and SIGINT support teams (SST)

MCWP 2-13
COORDINATING DRAFT

k. Theater Cryptologic Support Net (HF/UHF-SATCOM). Used to provide rapid exchange of cryptologic information with the cryptologic elements of other organizations. The communications path is provided by the supported commander, and the terminal equipment is provided by the radio battalion/SSU.

- w MAGTF (radio battalion/SSU)
- w Adjacent Service cryptologic elements
- w National cryptologic agencies
- w Joint/ATF cryptologic agencies

l. Radio Battalion CRITICOMM Net (UHF-SATCOM/HF/VHF). Used to provide CRITICOMM facilities to battalion elements that are physically removed from the CP in support of MAGTF units. The communications path is provided by the supported commander, and the equipment and personnel are provided by the radio battalion.

- w Radio battalion OCAC
- w Radio battalion/SSU CCE (at least two)

m. Radio Battalion/SSU Collection and Reporting Net (UHF-SATCOM/HF/VHF). Used to provide command and control and SIGINT reporting capabilities for battalion/SSU collection operations.

- w Radio battalion/SSU OCAC)
- w Deployed collection/direction funding (DF) SSTs

n. Radio Battalion/SSU EA Control Net (VHF). Used to provide the direction and control of radio battalion electronic countermeasures assets. The communications path, equipment, and personnel are provided by the radio battalion.

- w Radio battalion/SSU OCAC
- w Deployed EA teams

MCWP 2-13
COORDINATING DRAFT

o. Radio Battalion/SSU DF Flash Net (VHF). Used to provide the DF control station with a means of broadcasting DF flashes to the DF outstations. The communications path, equipment, and personnel are provided by the radio battalion.

w Radio battalion/SSU OCAC

w Deployed DF SSTs

p. Radio Battalion/SSU DF Report Net (VHF). Used for DF reporting from DF outstations to DF control. The communications path, equipment, and personnel are provided by the radio battalion.

w Radio battalion/SSU OCAC

w Deployed DF SSTs

q. DF Data Net (VHF). Used to exchange DF information between outstations and DF control. The communications path, equipment, and personnel are provided by the radio battalion.

w DF outstations/SSTs

w DF control (OCAC)

r. Tactical Receive Equipment and Related Applications Program Data Dissemination System (TDDS). Used to provide global surveillance information in time for sensor cueing and to provide indications and warning. Data is forwarded from sensor to communications gateways/relays for dissemination to worldwide military users via geosynchronous UHF satellite links. TDDS data sources include national and tactical sensor systems.

w Intelligence agencies

w IOC

w OCAC

w SSES

w ATFIC

w ACE/VMAQ squadron

MCWP 2-13
COORDINATING DRAFT

s. On-Board Processor/Direct Downlink (OBP/DDL). Used to distribute nationally generated data to operational forces and commanders worldwide. The information delivered directly to tactical users can be used to support indications and warning, surveillance, targeting (including OTH targeting), maneuver, execution, and battle damage assessment.

w Intelligence agencies

w IOC

w OCAC

w SSES

w ATFIC

w ACE/VMAQ squadron

t. TACINTEL Broadcast Service (TIBS). Used to provide near-real-time intelligence from an open network of interactive participants by using multiple sensors and sources. The TIBS broadcast uses UHF SATCOM assets for network operation and for the relay of out-of-theater specific information into the tactical users' AOs. TIBS participants include a wide variety of national and Service airborne, surface, and subsurface intelligence platforms.

w JTF, theater, and national intelligence organizations

w IOC

w OCAC

w SSES

w ATFIC

w ACE/VMAQ squadron

MCWP 2-13
COORDINATING DRAFT

u. Tactical Reconnaissance Intelligence Exchange System (TRIXS). Used to provide high-accuracy targeting data to multi-Service/joint Services command, control, and intelligence users. The TRIXS network supports full-duplex data and half-duplex voice connectivity between user terminals. It is designed to provide in-time intelligence reports that are focused on high-payoff ground threat targets. It is capable of providing maneuver, threat avoidance, targeting, mission planning, and sensor cueing support to commanders at all echelons. The TRIXS network can accept input from up to five intelligence producers (such as the Army Guardrail Common Sensor and Airborne Reconnaissance Low).

- w JTF, theater, and national intelligence organizations
- w IOC
- w OCAC
- w SSES
- w ATFIC
- w ACE/VMAQ squadron

v. TACINTEL Net. Used for transmission and reception of sensitive information sensor data and voice among collection and reporting units and detachments of the radio battalion, the MAGTF, and shipboard facilities, TACINTEL is an automated, high-speed data link.

- w JTF, theater, and national intelligence organizations
- w Radio Bn/SSU OCAC
- w SSES

w. Rad Bn/SSU Mission Equipment Control Data Link (MECDL) Net (UHF). Used to control, coordinate, and monitor the mission equipment of the MEWSS. This net is used for internal MEWSS operations and for interface and cooperative operation with the Army intelligence and EW common sensor systems.

- w MEWSS EA/SSTs
- w Army Guardrail Common Sensor
- w Army Ground-Based Common Sensor
- w Army Advanced Quickfix

MCWP 2-13
COORDINATING DRAFT

x. RadBn/SSU DF Net (UHF). Used to control, coordinate, and report DF data.

- w MEWSS EA/SST
- w Radio Bn/SSU OCAC
- w Army Technical Control and Analysis Element

y. RadBn/SSU Tasking and Reporting Net (VHF). Used to issue taskings/report results for RadBn elements employing the team portable collection system.

- w Analyst Subsystem
- w Collection outstations/SSTs

z. Radio Reconnaissance Command (UHF-TACSAT). Used for command and control of deployed RRTs; reporting of SIGINT collection and DF reports.

- w RadBn/SSU OCAC
- w ATFIC (SSES)
- w RRTs

aa. TROJAN SPIRIT II Net (C and Ku Band SATCOM). Used to receive, report, and disseminate intelligence information over a special-purpose satellite system.

- w MAGTF CE (CIC/IOC/OCAC)
- w ATFIC (SSES)
- w External intelligence agencies and organizations

bb. Force Reconnaissance Company Command (HF). Used to exercise command and coordinate administrative and logistic requests of subordinate units.

- w Force reconnaissance company reconnaissance operations center (ROC)
- w Subordinate units
- w *Liaison personnel*

MCWP 2-13
COORDINATING DRAFT

cc. Ground Sensor Platoon (GSP) Command (VHF). Used for command and control of GSP operations and for the coordination of GSP administrative and logistic support.

- w IOC (SARC/GSP liaison and control element)
- w GSP/detachment HQ
- w Monitoring sites/deployed sensor employment squad (SES)/sensor employment team liaison teams
- w *Others, as required*

dd. Sensor Reporting Net (VHF). Used as a means for rapid reporting of sensor data to supported units.

- w IOC (SARC (net control))
- w GSP monitoring sites
- w Supported units
- w *Others, as required*

ee. GSP Data Transmission (VHF). Used for transmission of sensor data collected by remote sensor sites.

- w GSP liaison and control element monitoring sites
- w IOC (SARC)
- w Remote sensor and sensor relay sites

ff. Counterintelligence/Human Intelligence (HUMINT) Team(s) Command (HF/VHF). Used for command and control of counterintelligence teams and subteams, interrogator-translator teams and subteams, and HUMINT exploitation teams operations and the coordination of counterintelligence/HUMINT administrative and logistic support.

- w IOC (SARC HUMINT liaison and control element)
- w Counterintelligence/HUMINT company/detachment command post
- w Deployed counterintelligence/HUMINT teams and HUMINT support teams (HST)
- w *Others, as required*

MCWP 2-13
COORDINATING DRAFT

gg. Counterintelligence/HUMINT Reporting Net (VHF). Used as a means for the rapid reporting of counterintelligence/HUMINT data to supported units.

- w IOC (SARC (net control))
- w Deployed counterintelligence/HUMINT teams and HSTs
- w Supported units
- w *Others, as required*

MCWP 2-13
COORDINATING DRAFT

2. Ground Combat Element Intelligence and Reconnaissance Radio Nets

a. Division/GCE Ground Reconnaissance Company Command (HF/VHF). Used for command and control of ground reconnaissance operations and for reporting reconnaissance information from deployed reconnaissance elements/teams to the GCE G-2/S-2 (SARC).

- w GCE HQ (G-2/S-2/SARC)
- w Reconnaissance units
- w LAR units
- w UAV squadron/detachment

b. Division/GCE Intelligence (HF/VHF). Used to provide rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations.

- w GCE HQ (G-2/S-2 intelligence operations)
- w Infantry units HQs
- w Artillery units HQs
- w Reconnaissance units
- w LAR units HQs
- w Tank units HQs
- w Assault amphibian units HQs
- w Combat engineer units HQs
- w Attached/direct support intelligence units (radio battalion SSU, CI/IT teams and HSTs)
- w UAV squadron/detachment (remote receive station)
- w *Attached combat and combat support units*

MCWP 2-13
COORDINATING DRAFT

c. Marine Division Defense Special Security Communications System Entry (UHF-SATCOM/HF/MUX). Used to provide the division commander with an SCI data communication capability with external agencies. The communications path is provided by the communications company, and the terminal equipment and personnel are provided by the division SSCT.

w SSCT

d. LAR Battalion/Company/Platoon Tactical 1 (VHF/HF). Used to exercise command and control of subordinate units. Each echelon has its own tactical command (TAC) net.

w Unit HQ

w Subordinate units and vehicles

w Recovery vehicles (company net)

w Liaison personnel

w Attached units

e. LAR Battalion Command (HF/VHF). Used to exercise command and coordinate administrative and logistic support.

w Battalion HQ

w Company HQs

w Liaison personnel

w *Supporting/attached units*

f. LAR Battalion Mortar (VHF). Used to request and control the fires of the mortar platoon.

w Forward observer teams

w Mortar platoon FDC

w Mortar representative at the battalion HQ

MCWP 2-13
COORDINATING DRAFT

g. Reconnaissance Battalion Command (HF/VHF). Used to exercise command and coordinate administrative and logistic support.

- w Recon Bn ROC
- w Subordinate units
- w Patrols/support aircraft/vehicles
- w *Supporting units*
- w Liaison teams at supported units

h. Infantry Regiment Intelligence (VHF). Used for rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations.

- w Infantry regiment HQ
- w Infantry battalion HQs
- w Intelligence units (radio battalion SSU, CI/IT teams, HST)
- w *Supporting and attached units*
- w *Regimental observation post*

i. Scout-Sniper Command (VHF). Used to exercise command and control of battalion scout-sniper operations and to report reconnaissance information collected by deployed scout-sniper teams.

- w Battalion S-2, S-3 and FSC
- w Scout-sniper teams

j. Artillery Regiment Radar Telling (VHF). Used to exchange radar intelligence information and for requests for surveillance of enemy counterfire weapons. May also be used for registration and adjustment of artillery fire.

- w Artillery regiment HQ
- w Countermortar radar sites
- w *Artillery battalions and batteries*

MCWP 2-13
COORDINATING DRAFT

k. Artillery Regiment Survey/Metro (VHF). Used to exchange survey, meteorological, and ballistic information and data between survey teams and artillery units.

- w Artillery regiment HQ
- w Artillery battalions/batteries
- w Survey officers and teams
- w *Division main command post*

MCWP 2-13
COORDINATING DRAFT

5. Aviation Combat Element Nets. MAW intelligence, reconnaissance and other select radio nets that are replaced by static MUX circuits will remain available as backups.

a. Antiaircraft Control (HF/VHF/MUX). Used to control surface-to-air missile (SAM) batteries. Types of information passed on this net include: target assignments, fire direction orders, weapons status commands, battery status reports, and progress-of-engagement reports.

w TAOC(s)

w EW/C

w LAAD Battery CP/ADCP

b. Antiaircraft Intelligence (HF/MUX). Used by SAM batteries to report targets acquired by the battery surveillance radar. TAOC passes selected early warning contacts to missile firing units. Combined with the antiaircraft control net when MUX is not available.

w TAOC(s)

w Air defense fire units

w EW/C

w LAAD Battery CP/ADCP

MCWP 2-13
COORDINATING DRAFT

c. Combat Information/Detection (HF/MUX). Used to report unidentified or hostile aircraft, including initial contact reports, tracking, amplifying, and final disposition. Multiple combat information/detection nets may be established for multiple TAOCs.

- w TAOC(s)
- w Early warning/control activities
- w LAAD Battery CP/ADCP
- w Air defense fire units
- w DASC (as required)
- w MATCD (as required)
- w TACC/TADC
- w *Other reporting agencies*

d. Ground-Based Data Link (VHF). Used for air defense CP downlink of surveillance information to short-range firing units.

- w ADCP
- w Short-range air defense
- w Remote sensors

e. Tactical Air Request/Helicopter Request (TAR/HR) (UHF-SATCOM/HF/VHF). Used by forward ground combat units to request immediate air support from the DASC. Intermediate ground combat echelons (FSCCs) monitor this net and may modify or disapprove a specific request. The DASC uses the net to brief the requesting unit on the details of the mission. Target damage assessments and HRs may be passed over this net. Multiple TAR/HR nets may be required, depending on the scope of close air support operations.

- w DASC
- w TACPs
- w HDC
- w TAOC
- w *Tactical air coordinator (airborne)*
- w *Forward air controller (airborne)*

MCWP 2-13
COORDINATING DRAFT

f. Defense Meteorological Satellite Program Satellite Imagery (SATCOM). Used as an encrypted receive-only circuit to provide a direct readout of real-time satellite imagery from polar orbiting satellites of the Defense Meteorological Satellite Program.

w Deployed Marine wing support squadron (MWSS)

g. Fleet Multichannel Broadcast (UHF SATCOM). Used as a receive-only circuit on channels 8 or 15 (environmental channels) of the satellite to provide weather bulletins produced by Navy regional centers.

w Broadcast from NCTAMS

w Deployed MWSS

h. Goldwing Communications (HF). Used as a secure, in-theater, joint net that may be used for voice traffic but is primarily for transmitting and receiving alphanumeric weather data.

w Other-Service meteorological and oceanographic agencies

w Deployed MWSS

i. Pilot to Metro (UHF). Used for exchange of meteorological information.

w Flying aircraft

w Weather detachment at EAF

j. Tactical Alert (HF). Used for rapid dissemination of air-raid warnings.

w MAGTF HQ

w GCE/ACE/CSSE HQ

w Air control agencies

MCWP 2-13
COORDINATING DRAFT

k. Television Infrared Observation Satellites Imagery (SHF). Used as an unencrypted receive-only circuit to provide a direct readout of real-time satellite imagery from the National Oceanographic Atmospheric Administration.

w Deployed MWSS

l. Weather Radar Net (AN/FPS-106). Used as a single-site radar that provides a visual depiction of precipitation and storm structure within a 200-nautical-mile radius of its location.

w Deployed MWSS at the EAF

m. Wing Intelligence (HF). Used for rapid reporting and dissemination of intelligence information.

w ACE G-2

w MAG S-2s

w Squadron S-2s

n. MAW Defense Special Security Communications System Entry (UHF-SATCOM/HF/MUX). Used to provides the wing commander with an SCI data communication capability with external agencies. The communications path is provided by the communications company, and the terminal equipment and personnel are provided by the MAW SSCT.

w SSCT

o. UAV Command Net (HF/VHF/UHF). Used to coordinate UAV activities.

w UAV squadron/detachment HQ

w GCS

w Launch and recovery site

w Remote video terminal teams

MCWP 2-13
COORDINATING DRAFT

p. UAV Primary Uplink Control (G-Band). Used to control air vehicle and payload.

- w Ground data terminal
- w Launch and recovery
- w Air vehicle

q. UAV Secondary Uplink Control (G-Band). Used to control air vehicle and payload if primary link control is lost.

- w Ground data terminal
- w Launch and recovery
- w Air vehicle

r. UAV Telemetry Downlink (G-Band). Used to provide real-time video display of target area and downlink flight control data.

- w GCS
- w Launch and recovery site
- w Remote video terminal teams
- w Air vehicle

s. Tactical Digital Information Link A (HF/UHF). TADIL-A, also called Link-11, is used to exchange tactical data in real time among ships, aircraft, and shore sites. TADIL-A messages provide navigational data, surface and subsurface tracks, and operational orders. TADIL-A is an encrypted half-duplex system. It can be used on either H single- or dual-sideband or UHF frequencies. The exchange of digital information by TADIL-A is accomplished by net-configured participating units (PUs) under the control of a net control station (NCS). A net can be composed of as few as two PUs.

- TAOC
- TACC
- VMAQ squadron/TERPES

MCWP 2-13
COORDINATING DRAFT

t. Tactical Digital Information Link B (VHF/UHF/SHF Multichannel Radio). TADIL-B, multichannel radio (MUX), (also known as Link-11B) is a full-duplex, point-to-point, encrypted system that simultaneously exchanges tactical data between two units capable of TADIL-B. TADIL-B messages provide navigational data, surface and subsurface tracks, and operational orders. Participants on a TADIL-B network, such as TERPES, are called reporting units (RUs). Some RUs are capable of simultaneously linking with several other RUs. Those units that can redistribute the information received from one RU to another RU are called forwarding.

- TACC
- TAOC
- MATCD
- VMAQ squadrons/TERPES

u. Voice Product Net (UHF). The VPN provides a communications means for forwarding nondigital intelligence information to other intelligence and operations elements.

- TACC
- TAOC
- EA-6B aircraft
- VMAQ squadron/TERPES
- *Other MAGTF external platforms (e.g., Rivet Joint, Compass Call, EP-3).*

MCWP 2-13
COORDINATING DRAFT

6. Combat Service Support Element Nets

a. CSS Alert/Broadcast (HF). Used for alert warning or general traffic pertaining to all (or a majority) of the units. Messages not of an alert warning type will be consecutively numbered at the time of transmission.

- w Unit HQ
- w General support group
- w Direct support group
- w CSS detachments

b. FSSG/CSSE Intelligence (HF/VHF). Used to provide rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing and supporting intelligence and reconnaissance operations.

- w CSSE HQ (G-2/S-2 intelligence operations)
- w CSSD combat service support operations centers

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

Appendix J

Intelligence Reports Dissemination Matrix Format

Purpose. This appendix provides an example of an intelligence reports matrix, used to ensure MAGTF-wide understanding and efficiency in dissemination of intelligence reports. It may be used as an exhibit to Tab E (Intelligence Reports) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence).

INTEL REPORT	ORIGIN	DISSEMINATION METHOD	VIA	COMMS PATH	MEF G2/IOC FILTER
I MEF ORGANIC					
EA-6B					
- TACELINTS	VMAQ	Printer (Primary)/ IAS (secondary)	VMAQ/TERPES	S-TDN	SARC; OCAC (alt)
AIR RECON					
-INFLT RPTS	All A/C	LAN	TACC/MAW	S-TDN	SARC; P&A Cell (alt)
		DSVT	TACC/MAW	Phone	SARC; P&A Cell (alt)
-MISREPS	All A/C	LAN	TACC/MAW	S-TDN	SARC; P&A Cell (alt)
		DSVT	TACC/MAW	Phone	SARC; P&A Cell (alt)
F/A-18D (ATARS)					
-IPIRS	VMFA	Printer (Primary)/ IAS (secondary)	TACC/MAW	S-TDN	SARC; P&A Cell (alt)
UAV					
-INFLTRPTS	VMU	Printer (Primary)/ IAS (secondary)		S-TDN	SARC
		DSVT		Phone	SARC
FORRECON					
-SALUTE RPTS; all other grnd recon rpts	Recon Teams	Printer/LAN	ROC	S-TDN	SARC
		DSVT	ROC	Phone	SARC
GSP					
-SENREPS		Printer/LAN			SARC
		DSVT		Phone	SARC
RADIO BN					
-TACREPS	SIGINT Spt Teams	Printer (Primary)/ JDISS (secondary)	OCAC	SCI-TDN	OCAC; P&A Cell
CI REPORTS					
Various CI Reporting	CI Teams and HSTs	LAN	CI HUMINT Co CP	S-TDN	SARC
		DSVT		Phone	
ITT REPORTS					
Various ITT Reporting	IT Teams and HSTs	LAN	CI/HUMINT Co. CP	S-TDN	SARC
		DSVT	CI/HUMINT Co. CP	Phone	SARC

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

INTEL REPORT	ORIGIN	DISSEMINATION METHOD	VIA	COMMS PATH	MEF G2/IOC FILTER
THEATER/JOINT					
JOINT STARS					
-RECCEXREPS	JSTARS aircraft	LAN; Printer (Primary)/IAS (secondary)	CGS	4 wire/ KG-84A	SARC; P&A Cell
U2R SYERS					
-RECCEXREPS	U2R	Printer (Primary)/ IAS (secondary)		4 wire/ KG-84A	SARC
-IPIRS	U2R	Printer (Primary)/ IAS (secondary)		4 wire/ KG-84A	SARC
U2R EMTI					
-RECCEXREPS (MTI)	U2R	Printer (Primary)/ IAS (secondary)		4 wire/ KG-84A	SARC; IIP (alt)
U2R ASARS					
-RECCEXREPS	U2R	Printer (Primary)/ IAS (secondary)		4 wire/ KG-84A	SARC; IIP (alt)
-IPIRS	U2R	Printer (Primary)/ IAS (secondary)		4 wire/ KG-84A	SARC; IIP (alt)
U2R SIGINT					
-TACREPS	U2R	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
-TACELINT	U2R	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
RC-135 SIGINT					
-TACREPS	RC-135	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
-TACELINT	RC-135	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
EP-3					
-TACREPS	EP-3	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
-TACELINT	EP-3	Printer (Primary)/ IAS (secondary)	OCAC	JWICS; Broadcast	OCAC
REEF POINT					
-IPIRS			OCAC	SI	SARC; OCAC (alt)
-TACREPS			OCAC	SI	SARC; OCAC (alt)
F-14 TARPS					
-IPIRS	CVBG	Printer (Primary) / IAS (secondary)		S-TDN	SARC
INTEL REPORT	ORIGIN	DISSEMINATION	VIA	COMMS	MEF G2/IOC FILTER

**MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT**

6/5/00

		METHOD		PATH	
NATIONAL					
Imagery Products	Various	Printer (Primary) / IAS (secondary)	MCISU or IIP	JWICS; SIPRNET	IIP; P&A Cell (alt)
-IPIR	Various	Printer (Primary) / IAS (secondary)	MCISU or IIP	JWICS; SIPRNET	IIP; P&A Cell (alt)
-IR	Various	Printer (Primary) / IAS (secondary)	MCISU or IIP	JWICS; SIPRNET	IIP; P&A Cell (alt)
-TACREP	Various	Printer (Primary) / IAS (secondary)	MCISU or IIP	Phone/IAS	OCAC
-TACELINT	TACSIM (SI)	Printer (Primary) / IAS (secondary)	OCAC	Phone/IAS	OCAC
-TACELINT	GALE Lite	TRAP	OCAC	Phone/IAS	OCAC
EPW/CI/HUMINT					
-Various Reporting	J2X; others	Printer (Primary)/ IAS (secondary)	CI/HUMINT Co. CP	SIPRNET	SARC
REPORTS					
-INTSUMS	External	LAN/IAS	P&A Cell	SIPRNET	P&A Cell
	Internal	LAN Homepage	P&A Cell	S-TDN	P&A Cell
-INTREPS	External	LAN/IAS	P&A Cell	SIPRNET	P&A Cell
	Internal	LAN Homepage	P&A Cell	S-TDN	P&A Cell
-RRFIs		LAN/IAS	P&A Cell	JWICS; SIPRET alt	P&A Cell; SARC (alt)
-TARGET LIST	P&A Cell	IAS/RAAP	P&A Cell	S-TDN or SIPRNET	P&A Cell
-Consolidated BDA (First Phase)	P&A Cell	IAS	P&A Cell	S-TDN or SIPRNET	P&A Cell

Appendix K

MAGTF Intelligence Dissemination Plan Format

Purpose. Tab C (Intelligence Dissemination Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) should explain how intelligence dissemination elements under the command or supporting the MAGTF will be used to support this plan. Additionally, it provides basic guidance and direction to subordinate commanders and intelligence officers for the conduct of MAGTF intelligence dissemination operations and the support of intelligence elements and personnel identified to fulfill the intelligence dissemination requirements in support of this plan.

CLASSIFICATION

Copy no. __ of __ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

Tab C to APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B
(INTELLIGENCE) TO MAGTF OPORD X ()
Intelligence Dissemination Plan (U)

() **REFERENCES:** Identify organic DoD, DIRNSA, NIMA, and other directives; combatant commander, JTF, JFMCC/JFLCC/JFACC or other higher authorities' operations orders, tactics, techniques, and procedures (TTP), and standard operating procedures (SOP) for intelligence dissemination operations; formats; and any other relevant documents that pertain to anticipated intelligence dissemination operations.

1. () **SITUATION**

a. () **Define the Area of Operations (AO) and Area of Interest (AOI).** Describe the limits of the AO and AOI. Summarize pertinent weather, terrain, and other AO characteristics and conditions as they may influence the conduct of intelligence dissemination operations.

b. () **Enemy.** Refer to Annex B (Intelligence) and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence dissemination operations.

c. () **Assigned MAGTF Organic and Supporting Intelligence Dissemination Assets.**
Identify organic and supporting forces available to perform intelligence dissemination functions.

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

d. () Assumptions. (Derived during the mission analysis step of the Marine Corps planning process.)

e. () Intelligence Dissemination Considerations. List key intelligence dissemination, CIS and interoperability considerations which impact this OPLAN or OPORD.

(1) () Availability of national and commercial intelligence and multi-purpose CIS resources.

(2) () Intelligence C2 and dissemination support to and from JTF/Component Headquarters and other external commands and intelligence organizations.

(3) () Creation and manning of forward intelligence C2 and operations elements.

2. () **MISSION**. State concisely the intelligence dissemination mission as it relates to the command's planned operations.

3. () **EXECUTION**

a. () Concept of Operations. Summarize pertinent command relationships, task-organization, main and supporting efforts, and the scope of MAGTF and supporting intelligence dissemination operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations Plan) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to intelligence operations. Outline the purpose and concept of intelligence dissemination operations, specified priorities, and summarize the means and agencies to be employed to support the operations and intelligence concepts of operations. Address the integration of JTF, other components, theater, national, and allied forces' intelligence operations, dissemination, and CIS support.

b. () Dissemination Tasks for Intelligence Units and Organizations, Subordinate Units, and Detachment Commanders/OICs.

(1) Orders to Subordinate, Attached, and Supporting Units. Use separate subparagraphs to list detailed instructions for each unit conducting intelligence-related dissemination operations, including the originating headquarters, subordinate commands, and separate intelligence support units.

(a) () Marine Division(s)

(b) () Marine Aircraft Wing(s)

(c) () Force Service Support Group(s)

MCWP 2-13, *MAGTF Intelligence Dissemination*
COORDINATING DRAFT

6/5/00

(d) () Commanding Officer, Intelligence Battalion/Intelligence Support
Coordinator

1 () OIC, Support Cell

2 () OIC, Production & Analysis Cell

3 () OIC, Surveillance and Reconnaissance Cell

4 () Intelligence Systems Officer

5 () Commanding Officer, CI/HUMINT Company

6 () Platoon Commander, Imagery Intelligence Platoon

7 () Platoon Commander, Topographic Platoon

8 () OIC, Joint STARS Common Ground Station

(e) () Commander, Marine Corps Imagery Support Unit (if tasked to support)

(f) () Commanding Officer, VMU Squadron

(g) () Commanding Officer, VMAQ Squadron

(h) () Commanding Officer, Radio Battalion

(i) () Commanding Officer, Force Reconnaissance Company

(j) () OIC, National Intelligence Support Team (if attached)

(2) () Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached, or supporting and from which intelligence CIS support is requested, including other components, JTF headquarters, allied or coalition forces, theater, and national operational and intelligence elements.

c. () Coordinating Instructions. Reference Appendix 16 (Intelligence Operations Plan), Annex K (CIS), Annex J (C2), and command and other pertinent forces' and organizations' intelligence and counterintelligence SOPs. Detail here or in supporting tabs key changes to unit SOPs. Additional topics to include or emphasize here are: requesting CIS and dissemination support, timely reporting procedures for intelligence CIS problems, coordinating switchover to backup dissemination paths, intelligence operations, C2, and CIS hand over between command echelons, etc.

(1) () General Dissemination Guidance and Procedures. Use separate subparagraphs

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

to list detailed instructions for routine and time-sensitive dissemination, precedence of transmissions, predetermined recipient lists, general and specific broadcast parameters, reporting thresholds and reporting filters.

(2) () Intelligence Reporting Criteria

(3) () Resource Allocation. Discuss dissemination resource allocation between both the main and supporting efforts, and between support to current operations and support to future operations.

(4) () Intranet Management. List detailed instructions for homepage and database management, to include authorities for posting, updating, and removing information and intelligence.

(5) () Common Operational Picture/Common Tactical Picture. List detailed instructions for track data and auto-forwarding, broadcast times, and boundary/track ownership responsibilities.

(6) () Formats and Standardization. Provide formats for internal and external MAGTF intelligence dissemination and reporting, preformatted templates, and/or where to find these referenced elsewhere in the OPLAN. Include standards and limits on size and composition of files attached to e-mail.

4. () **ADMINISTRATION AND LOGISTICS**

a. () Logistics. Reference Annex D (Logistics). Identify intelligence dissemination logistics requirements and concerns, such as: unique combat service support requirements (batteries, unique replacement parts), procedures, and other guidance to support MAGTF intelligence units and operations; procedures for specialized technical logistics support necessary from external organizations; map distribution; requirements for courier runs; etc.

b. () Personnel. Identify personnel requirements and concerns that affect intelligence dissemination operations and support (systems administrators, global sourcing requirements, etc.).

5. () **COMMAND AND CONTROL**

a. () Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding MAGTF command relationships that will influence intelligence operations and dissemination support.

b. () Information Management. Reference Annex U (Information Management), Annex C (Operations) and Appendix 16 (Intelligence Operations Plan). Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence

MCWP 2-13, MAGTF Intelligence Dissemination
COORDINATING DRAFT

6/5/00

databases, reports, etc.) that will influence MAGTF intelligence dissemination, reporting, and other operations.

c. () Communications and Information Systems. Reference Appendix 16 (Intelligence Operations Plan) and Annex K (CIS). Provide any instructions necessary regarding CIS that will influence MAGTF intelligence dissemination operations. List intelligence dissemination priorities (by operational phase, intelligence units, intelligence operations and C2 nodes, intelligence activities – whichever approach is most effective for the operation).

d. () Intelligence C2 Nodes and Facilities. Reference the unit's SOP and Appendix 16 (Intelligence Operations Plan). Provide any guidance and instructions necessary regarding establishment and operation of intelligence C2 nodes and facilities and dissemination support and priorities to these, to include, at a minimum: G/S-2 elements within future plans, future operations, current operations, and force fires centers; IOC's Support Cell, SARC and P&A Cell; CI/HUMINT Company CP; reconnaissance operations center; OCAC; command element tactical or rear echelons; and intelligence liaison elements.

Tabs (as required)

A Intelligence Dissemination Flow Diagram(s) (See figure 4-1 for one example.)

B Intelligence Dissemination Requirements Matrix (See figure 4-2 for one example.)